ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Σχεδιασμός Εργαλείου Ανίχνευσης Επιθέσεων σε FlexRay για Ευφυή και Συνδεδεμένα Οχήματα

Διπλωματική Εργασία

Σίσκος Δημήτριος

Επιβλέπων: Μούντανος Ιωάννης

Σεπτέμβριος 2023

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Σχεδιασμός Εργαλείου Ανίχνευσης Επιθέσεων σε FlexRay για Ευφυή και Συνδεδεμένα Οχήματα

Διπλωματική Εργασία

Σίσκος Δημήτριος

Επιβλέπων: Μούντανος Ιωάννης

Σεπτέμβριος 2023

UNIVERSITY OF THESSALY

SCHOOL OF ENGINEERING

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

Design of an Attack Detection Tool in FlexRay for Intelligent and Connected Vehicles

Diploma Thesis

Siskos Dimitrios

Supervisor: Moudanos Ioannis

September 2023

Εγκρίνεται από την Επιτροπή Εξέτασης:

Επιβλέπων	**Μούντανος Ιωάννης** Αναπληρωτής Καθηγητής, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Πανεπιστήμιο Θεσσαλίας
Μέλος	**Χούστης Ηλίας** Ομότιμος Καθηγητής, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Πανεπιστήμιο Θεσσαλίας
Μέλος	**Χρήστος Δ. Αντωνόπουλος** Καθηγητής, Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Πανεπιστήμιο Θεσσαλίας

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΠΕΡΙ ΑΚΑΔΗΜΑΪΚΗΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΚΑΙ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα διπλωματική εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελούν αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλουν οποιασδήποτε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχουν έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Δηλώνω επίσης ότι τα αποτελέσματα της εργασίας δεν έχουν χρησιμοποιηθεί για την απόκτηση άλλου πτυχίου. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο Δηλών

Σίσκος Δημήτριος

DISCLAIMER ON ACADEMIC ETHICS AND INTELLECTUAL PROPERTY RIGHTS

Being fully aware of the implications of copyright laws, I expressly state that this diploma thesis, as well as the electronic files and source codes developed or modified in the course of this thesis, are solely the product of my personal work and do not infringe any rights of intellectual property, personality and personal data of third parties, do not contain work / contributions of third parties for which the permission of the authors / beneficiaries is required and are not a product of partial or complete plagiarism, while the sources used are limited to the bibliographic references only and meet the rules of scientific citing. The points where I have used ideas, text, files and / or sources of other authors are clearly mentioned in the text with the appropriate citation and the relevant complete reference is included in the bibliographic references section. I also declare that the results of the work have not been used to obtain another degree. I fully, individually and personally undertake all legal and administrative consequences that may arise in the event that it is proven, in the course of time, that this thesis or part of it does not belong to me because it is a product of plagiarism.

The Declarant

Siskos Dimitrios

Ευχαριστίες

Πρωτίστως, θέλω να ευχαριστήσω τον επιβλέποντα της διπλωματικής εργασίας μου, καθηγητή κ. Ιωάννη Μούντανο, για την πολύτιμη καθοδήγησή του και την εμπιστοσύνη που μου έδειξε αναθέτοντάς μου το συγκεκριμένο θέμα. Ευχαριστώ ιδιαιτέρως τον αδερφό μου Διονύση για την υποστήριξή του σε όλη την διάρκεια εκπόνησης της εργασίας μου και για την πολύτιμη βοήθειά του. Πάνω απ' όλα, είμαι ευγνώμων στους γονείς μου, Αθανάσιο και Μελπομένη για την ολόψυχη αγάπη και υποστήριξή τους όλα αυτά τα χρόνια. Αφιερώνω αυτήν την εργασία στη γιαγιά μου.

Διπλωματική Εργασία

Σχεδιασμός Εργαλείου Ανίχνευσης Επιθέσεων σε FlexRay για Ευφυή και Συνδεδεμένα Οχήματα

Σίσκος Δημήτριος

Περίληψη

Σκοπός της παρούσας εργασίας είναι ο σχεδιασμός ενός εργαλείου ανίχνευσης επιθέσεων σε FlexRay για ευφυή και συνδεδεμένα οχήματα, για εφαρμογές σε εγκληματολογικές έρευνες και στην αποτροπή κακόβουλων ενεργειών σε πραγματικό χρόνο στο επίπεδο διασύνδεσης των δεδομένων του δικτύου. Για την επίτευξη αυτού, σχεδιάστηκε ένα λογισμικό, FlexRayGen, που προσομοιώνει τη επικοινωνία δύο κόμβων με το πρωτόκολλο FlexRay πάνω στο δίκτυο. Το πρόγραμμα αυτό, είναι υπεύθυνο και για την υλοποίηση των διαδικασιών κατασκόπευσης της επικοινωνίας και της εφαρμογής επιθέσεων. Για την οπτική απεικόνιση των διαδικασιών και λειτουργιών υλοποιήθηκε το λογισμικό FlexRayShark που προβάλλει στον χρήστη όλη την κίνηση στο δίκτυο, τις ενέργειες που πραγματοποιούνται και των πληροφοριών που δέχεται και αποστέλλει ένας κόμβος κάθε χρονική στιγμή. Τέλος όλη η προβαλλόμενη και μη πληροφορία προσομοίωσης συλλέγεται και αναλύεται από τους αλγορίθμους του εργαλείου ανίχνευσης, προκειμένου να διαπιστωθεί η ύπαρξη ή μη κακόβουλων ενεργειών. Εκτελούνται συγκεκριμένα πειράματα των οποίων η μέθοδος, τα αποτελέσματα και τα συμπεράσματα παρουσιάζονται αναλυτικά. Τέλος προτείνονται συγκεκριμένες κατευθύνσεις για την συνέχεια της μελέτης.

Λέξεις-κλειδιά:

FlexRay, Κυβερνοασφάλεια, Αυτοκινητοβιομηχανία, Εγκληματολογία Οχημάτων

Diploma Thesis

Design of an Attack Detection Tool in FlexRay for Intelligent and Connected Vehicles

Siskos Dimitrios

Abstract

The purpose of this work is to design an attack detection tool in FlexRay for intelligent and connected vehicles, for applications in forensics investigations and in preventing malicious actions in real time at the datalink layer of the network. To achieve this, a software, FlexRayGen, was designed that simulates the communication of two nodes with the FlexRay protocol over the network. This program is also responsible for the implementation of communication spying procedures and the application of attacks. For the visual display of the processes and functions, the FlexRayShark software was implemented that displays to the user all the traffic in the network, the actions that are carried out and the information that a node receives and sends at any given time. Finally, all projected and non-projected simulation information is collected and analyzed by the detection tool's algorithms, in order to determine the presence or absence of malicious actions. Specific experiments are carried out whose method, results and conclusions are presented in detail. Finally, specific directions are proposed for the continuation of the study.

Keywords:

FlexRay, Automotive, Cybersecurity, Vehicle Forensics

Πίνακας περιεχομένων

Κατάλογος εικόνων

Κατάλογος Διαγραμμάτων

Κατάλογος Πινάκων

Συντομογραφίες

AIDS Anomaly Based Intrusion Detection System

A3C Asynchronous Advance Actor Critic

CAN Control Area Network

CAS Collision Avoidance Symbol

CC Communication Controller

CHI Controller Host Interface

DoS Denial of Service

ECU Electronic Control Unit

FES Frame End Sequence

FFNN Feed Forward Neural Network

FSP Frame and Symbol Processing

FSS Frame Start Sequence

GATE General Architecture for Text Engineering

HIDS Host Based Intrusion Detection System

IDS Intrusion Detection System

ISOMAP Isometric Map

IVN In-Vehicle Network

kNN k Nearest Neighbors

LIDAR Light Detection and Ranging

LIN Local Connect Network

LLE Local Linear Embedding

LPM Linear Projection Method

LSTM Long Short-Term Memory

MCTS Monte Carlo Tree Search

MCU Microcontroller Unit

MitM Man-in-the-Middle Attack

MOST Media Oriented Systems Transport

NIDS Network Based Intrusion Detection System

NMV Network Management Vector

NPM Nonlinear Projection Method

NUA Node Under Attack

OBD-II On-Board Diagnosis

OTA Over-the-Air update

RF Random Forest

SIDS Signature Based Intrusion Detection System

SVC Support Vector Classification

SVM Support Vector Machine

SVR Support Vector Regression

TDMA Time Division Multiple Access

TD Temporal Difference

TPMS Tire Pressure Monitoring System

TSS Transmission Start Sequence

RBF Radial Basis Function

RNN Recurrent Neural Network

UART Universal Purpose Asynchronous

V2I	Vehicle to Infrastructure
V2N	Vehicle to Network
V2P	Vehicle to Pedestrian
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
ΕΣΟ	Ευφυές και Συνδεδεμένο Όχημα
ΗΜΕ	Ηλεκτρονική Μονάδα Ελέγχου
συν.	συνεργάτες
κ.ά.	και άλλα
κ.λπ.	και λοιπά
κ.ο.κ	και ούτω καθεξής

Κεφάλαιο 1 Εισαγωγή

Το αντικείμενο της διπλωματικής πραγματεύεται το θέμα της κυβερνοασφάλειας των σύγχρονων και κυρίως των μελλοντικών αυτόνομων οχημάτων. Σε μια εποχή, μόλις μερικών δεκαετιών που η τεχνολογική εξέλιξη, με την επανάσταση των υπολογιστών, ακμάζει - δημιουργούνται όλο και πιο έντονοι προβληματισμοί σχετικά με την ασφάλεια και την εμπιστοσύνη σ ’αυτήν. Η επικείμενη απότομη εισαγωγή στην ζωή των πολιτών της τεχνητής νοημοσύνης και του δικτύου των πραγμάτων, δεν μπορεί να αφήσει ανεπηρέαστη μία από τις μεγαλύτερες βιομηχανικές δραστηριότητες στον πλανήτη, αυτή της αυτοκινητοβιομηχανίας. Ηγέτιδα δύναμη σε πολλές τεχνολογικές εξελίξεις την φέρνει όλο και πιο κοντά στην καθημερινότητα του ανθρώπου. Η αυτόνομη οδήγηση, μια από τις επαναστάσεις στον κλάδο, αλλά και πολλές άλλες ανέσεις και λειτουργίες που υποστηρίζουν τα σύγχρονα οχήματα, εγείρουν προβληματισμούς σχετικά με την ακεραιότητα των προσωπικών δεδομένων και της ασφάλειας των χρηστών μέσα σ ’αυτά. Η ψηφιοποίηση των οχημάτων, προσφέρει ανεξάντλητες δυνατότητες αλλά ταυτόχρονα δημιουργεί κινδύνους. Η ανάδειξη ευπαθειών και κινδύνων έχει ενθαρρύνει τις κατασκευαστικές στην υιοθέτηση πολιτικών προσανατολισμένων στην ασφάλεια και αν συνεχιστεί θα οδηγήσει αναπόφευκτα στην ανάπτυξη και τον σχεδιασμό πιο ασφαλών ψηφιακά οχημάτων. Πέρα όμως από τους εύκολα προσκείμενους κινδύνους, μια βαθύτερη ανάλυση, που λαμβάνει υπόψιν τις νόρμες της σύγχρονης κοινωνίας, προκαλεί πολύ μεγαλύτερη ανησυχία. Λέξεις όπως «τρομοκρατία», «πόλεμος», «κατασκοπεία», «παραβίαση προσωπικών δεδομένων», «δημοσίευση χωρίς την συγκατάθεση ευαίσθητων δεδομένων», βρίσκονται καθημερινά στις πρώτες ειδήσεις όλων των μέσων μαζικής ενημέρωσης. Οι τεχνολογίες ενός ευφυούς και συνδεδεμένου οχήματος είναι εύκολο να υπηρετήσουν ή να υποστούν τέτοιους σκοπούς και ενέργειες αντίστοιχα, αν χρησιμοποιηθούν με κακόβουλες προθέσεις. Οφείλει λοιπόν η επιστημονική κοινότητα να στραφεί στον σχεδιασμό εργαλείων ικανών να διαπιστώνουν και να επιβεβαιώνουν τις ενέργειες αυτές. Κατά συνέπεια τη θωράκιση της κυβερνοασφάλειας των ευφυών και συνδεδεμένων οχημάτων πρέπει να ακολουθήσει η ανάπτυξη του κλάδου της εγκληματολογίας των οχημάτων (*automotive forensics*), προκειμένου να επιβεβαιώνεται η κακόβουλη δράση, όπως

έχει ήδη αναπτυχθεί σε άλλους τομείς, με χαρακτηριστικά παραδείγματα τις κινητές συσκευές και το διαδίκτυο.

1.1 Αντικείμενο της Διπλωματικής

Σκοπός της παρούσας εργασίας είναι να αναδείξει την σπουδαιότητα και την αναγκαιότητα για σχεδιασμό ασφαλών τεχνολογιών αυτοκίνησης. Στοχεύει να θέσει τα θεμέλια για την ανάπτυξη ενός περιβάλλοντος και ενός εργαλείου που θα εξυπηρετήσει την κυβερνοασφάλεια των ευφυών και συνδεδεμένων οχημάτων. Ο σχεδιασμός ενός εργαλείου ικανού να ανιχνεύει κυβερνοεπιθέσεις σε ένα από τα πιο διαδεδομένα και σύγχρονα πρωτόκολλα ενδοεπικοινωνίας μπορεί να αποτελέσει ασπίδα άμυνας αλλά και πολύτιμο διαπιστευτήριο στα χέρια των αρχών. Αδιαμφισβήτητη είναι η αξία της ύπαρξης ενός αξιόπιστου μηχανισμού ανίχνευσης επιθέσεων τέτοιου τύπου σε πραγματικό χρόνο, για την αποφυγή κακόβουλων δράσεων που μπορεί να οδηγήσουν σε ανθρώπινες απώλειες. Εξίσου όμως σημαντική κρίνεται και η διάθεση στις εξουσιοδοτημένες αρχές, που μελετούν ή αποτρέπουν εγκληματικές ενέργειες, ενός εργαλείου ικανού να εντοπίζει και να επιβεβαιώνει την δράση εγκληματικών ενεργειών.

1.1.1 Συνεισφορά

Η συνεισφορά της παρούσας διπλωματικής συνοψίζεται ως εξής:

1. Δημιουργείται ένα πρόγραμμα προσομοίωσης της επικοινωνίας με το πρωτόκολλο FlexRay ανάμεσα σε δύο κόμβους
2. Υλοποιείται δεύτερο πρόγραμμα που υπηρετεί την παρουσίαση και ανάλυση των αποτελεσμάτων στον χρήστη. Στην πραγματικότητα αποτελεί την γραφική διεπαφή με τον μελετητή.
3. Στο πρώτο λογισμικό εισάγεται ο μηχανισμός προσομοίωσης των κυβερνοεπιθέσεων
4. Σχεδιάζονται οι αλγόριθμοι και μοντέλα ανίχνευσης των επιθέσεων.
5. Τέλος εκτελούνται πειράματα και αναλύονται τα αποτελέσματα.

1.2 Οργάνωση Τόμου

Η διπλωματική χωρίζεται σε έξι κύριες ενότητες.

Στο Κεφάλαιο 2 γίνεται μια εισαγωγή στην βασική δομή και διάρθρωση των ευφυών και συνδεδεμένων. Αποσαφηνίζεται ο όρος και περιγράφονται οι τεχνολογίες και οι δυνατότητες που αυτά φέρουν. Συνεχίζει με την αρχιτεκτονική, τους λειτουργικούς τομείς και τις κύριες μονάδες. Παράλληλα γίνεται μια νύξη στις τοπολογίες των δικτύων και στα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται στην αυτοκινητοβιομηχανία. Το κεφάλαιο ολοκληρώνεται με την παρουσίαση των κινδύνων που εγκυμονούν και των μηχανισμών με τους οποίους μπορούν να εφαρμοστούν επιθέσεις.

Στο Κεφάλαιο 3 περιγράφεται συνοπτικά αλλά με ακρίβεια το πρωτόκολλο FlexRay. Επικεντρώνεται στους κύριους μηχανισμούς του και στη λεπτομερή παρουσίαση των σημείων που ήταν καθοριστικά στην διαδικασία της υλοποίησης. Δίνεται έμφαση στην αρχιτεκτονική των κόμβων και των δικτύων, στην δομή του πλαισίου και στον κύκλο επικοινωνίας. Κλείνει δίνοντας οι σχετικές πληροφορίες και για τον μηχανισμό μετάδοσης των μηνυμάτων.

Το Κεφάλαιο 4 περιλαμβάνει την ανάλυση των διανυσμάτων επίθεσης. Παρουσιάζονται οι πιο διαδεδομένες επιθέσεις και κατόπιν ταξινομούνται τα διανύσματα βάση του σκοπού του επιτιθέμενου. Επίσης γίνεται αναφορά στα entry point και παρατίθενται ορισμένες σημειώσεις για επιθέσεις συγκεκριμένα σε FlexRay. Η τελευταία ενότητα είναι αφιερωμένη στην ανάπτυξη μηχανισμών ανίχνευσης και την αξία της μηχανικής μάθησης σε αυτούς.

Το Κεφάλαιο 5 είναι αφιερωμένο στην προγραμματιστική υλοποίηση. Περιγράφει τις απαιτήσεις και τις παραδοχές που γίναν. Ιδιαίτερη έμφαση δίνεται στις σχετικές εργασίες και τα κριτήρια της επιλογής του μηχανισμού ανίχνευσης και των επιθέσεων. Πραγματοποιείται αναλυτική επεξήγηση του λογισμικού FlexRayGen και πως επιτυγχάνεται η προσομοίωση του FlexRay σε αυτό. Η ενότητα συνεχίζει με την παρουσίαση του λογισμικού FlexRayShark, που είναι ένα πρόγραμμα που βοηθά τον μελετητή στην απεικόνιση των δρώμενων εντός της προσομοίωσης και στην εξαγωγή χρήσιμων δεδομένων από αυτήν.

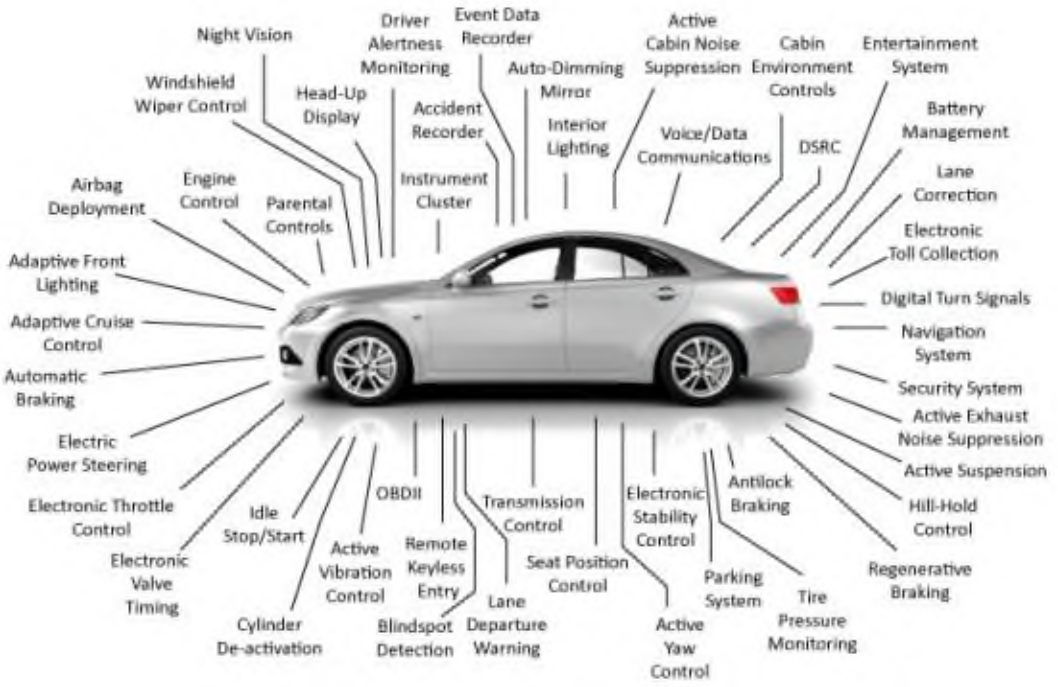
Το Κεφάλαιο 6 δίνει πληροφορίες για τα διαθέσιμα δεδομένα, την επεξεργασία αυτών και τα πειράματα που εφαρμόστηκαν. Ιδιαίτερη έμφαση, δίνεται στα αποτελέσματα και την αξιολόγηση τους.

Το Κεφάλαιο 7 αποτελεί μια σύνοψη της συνολικής μελέτης, των μεθόδων και λειτουργιών που αναπτύχθηκαν, των αποφάσεων που πάρθηκαν και των αποτελεσμάτων που τελικά παράχθηκαν. Υπογραμμίζονται συμπεράσματα που προκύπτουν από αυτήν και προτείνονται μελλοντικές κατευθύνσεις για την συνέχιση και επέκταση του έργου.

Κεφάλαιο 2 Ευφυή και Συνδεδεμένα Οχήματα

2.1 Εισαγωγή

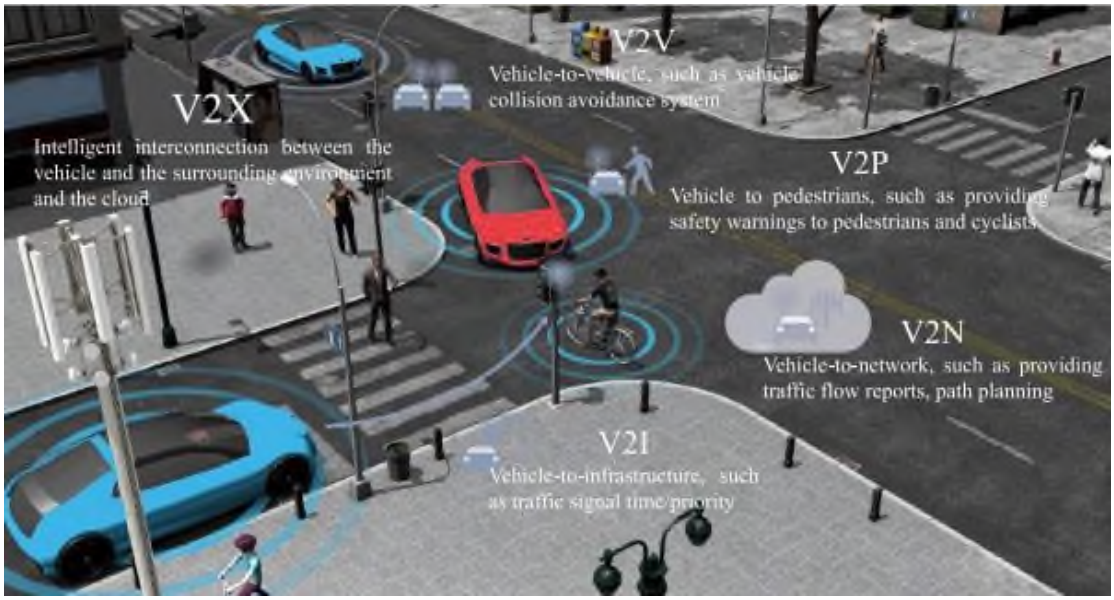
Τα ευφυή και συνδεδεμένα οχήματα (**Εικόνα 1**) αποτελούν οχήματα που συνδυάζουν τεχνολογίες αιχμής, όπως η τεχνητή νοημοσύνη, τα δεδομένα μεγάλου όγκου, τα ραντάρ μήκους κύματος χιλιοστού, η τεχνική ανίχνευσης φωτός και απόστασης LiDAR, οι κάμερες υψηλής ευκρίνειας βασισμένες σε πραγματικού χρόνου αντίληψη του περιβάλλοντος αλλά και αμέτρητες ακόμα φέρνοντας την επανάσταση στον τρόπο που πραγματοποιούνται οι μετακινήσεις.



Εικόνα 1 Παράδειγμα τεχνολογιών ενός ευφυούς και συνδεδεμένου οχήματος [20]

Η ειδοποιός διαφορά ενός ΕΣΟ από ένα κλασσικό όχημα, που το καθιστά τόσο μοναδικό και επαναστατικό, είναι αφενός η ευφυία και αφετέρου η συνδεσιμότητα. Ο όρος ευφυία αναφέρεται στην ικανότητα να συλλέγει μεγάλες ποσότητές δεδομένων, επικοινωνώντας και αλληλοεπιδρώντας με το περιβάλλον του, να τις αναλύει και να παίρνει αποφάσεις βάσει αυτών σε πραγματικό χρόνο. Η συνδεσιμότητα αφορά στην αξιοποίηση της δύναμης του διαδικτύου και των τεχνολογιών ασύρματης επικοινωνίας μέσω των οποίων καθίσταται δυνατή η άμεση επικοινωνία μεταξύ οχημάτων και μεταξύ οχημάτων - περιβάλλοντος. Στο περιβάλλον περιλαμβάνονται οι κυκλοφοριακές υποδομές, οι πεζοί, οι

κατασκευάστριες εταιρίες, οι σταθμοί φόρτισης ή τα πρατήρια καυσίμων και πολλά άλλα, που όλα μαζί σχηματίζουν ένα ισχυρό δίκτυο γνωστό ως οικοσύστημα «*V2X*» (**Εικόνα 2**). Αυτό το δίκτυο επιτρέπει την απρόσκοπτη ανταλλαγή πληροφοριών σχετικά με τις κυκλοφοριακές συνθήκες, τους οδικούς κινδύνους ακόμη και τον καιρό, επιτρέποντας την αποφυγή συμφόρησης, την εμπλοκή σε επικίνδυνες συνθήκες και την προσαρμογή της ταχύτητας, μεταμορφώνοντας έτσι την αστική κινητικότητα, βελτιστοποιώντας τη ροή της κυκλοφορίας, μειώνοντας τις εκπομπές και βελτιώνοντας την αποδοτικότητα των μεταφορών.



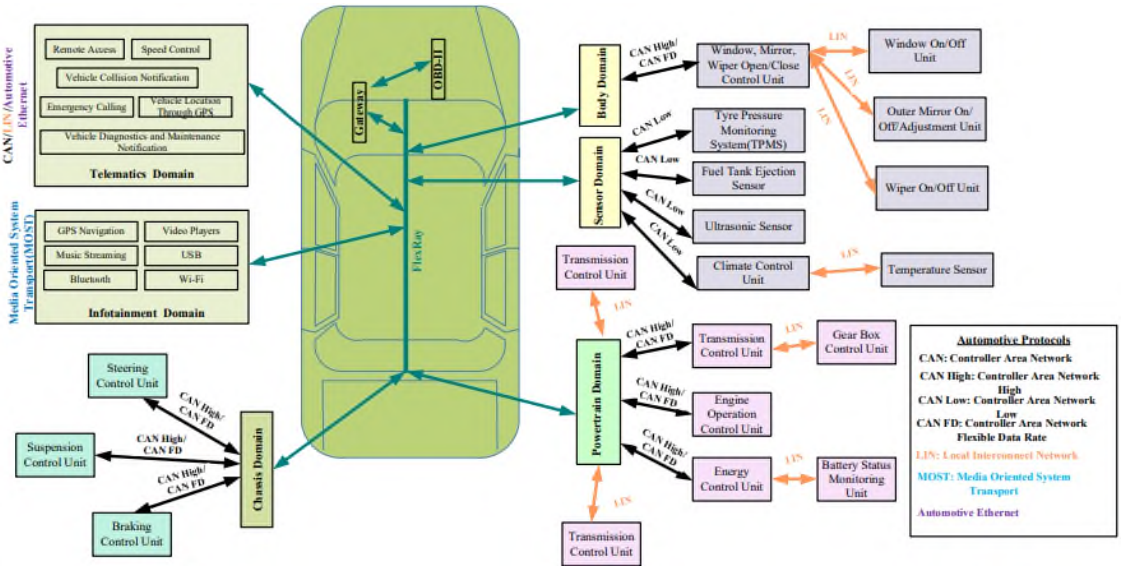
Εικόνα 2 Παράδειγμα δικτύου Vehicle to Everything (V2X) [19]

2.2 Αρχιτεκτονική

2.2.1 Αρχιτεκτονική Οχημάτων

Η ανάγκη για αυτονομία σε συνδυασμό με τις όλο αυξανόμενες απαιτήσεις των πελατών για άνεση και βελτίωση της οδηγικής εμπειρίας, έχει προκαλέσει την μαζική προσθήκη και εισαγωγή ηλεκτρονικών συστημάτων και στοιχείων στα οχήματα. Ταυτόχρονα η απόδοση και αξιοπιστία των σύγχρονων ηλεκτρονικών έχει επιτρέψει πλέον την χρήση τους ακόμα και σε κρίσιμα για την λειτουργία και την ασφάλεια του οχήματος συστήματα. Τα ενσωματωμένα συστήματα ενός ευφυούς και συνδεδεμένου οχήματος διακρίνονται σε κατηγορίες βάσει της λειτουργικότητας και των περιορισμών τους. Πεδία όπως αυτό του «*power train*», του σασί και τα ενεργητικά ή παθητικά συστήματα ασφαλείας μπορούν να χαρακτηριστούν ως πιο

προσανατολισμένα στο όχημα ενώ άλλα όπως τα πολυμέσα, τα τηλεματικά και της διεπαφής ανθρώπου μηχανής ως πιο ανθρωποκεντρικά. Η **Εικόνα 3** συνοψίζει όλη αυτήν την πληροφορία, η οποία αναλύεται εκτενέστερα αμέσως μετά.



Εικόνα 3 Λειτουργικοί τομείς ευφυούς και συνδεδεμένου οχήματος [25]

2.2.2 Λειτουργικοί Τομείς

Τα ηλεκτρονικά συστήματα ενός ευφυούς και συνδεδεμένου αυτοκινήτου διακρίνονται σε έξι κύριους τομείς, αυτόν του κινητήρα και της μετάδοσης «*Power Train Domain*», αυτόν του σασί «*Chassis Domian*», της τηλεματικής «*Telematics Domain*», των πολυμέσων και της ενημέρωσης «*infotainment Domain*», των αισθητήρων «*Sensors Domain*», του αμαξώματος «*Body Domian*» και τέλος της ενεργούς και παθητικής ασφαλείας «*Active/Passive Safety Domain*».

2.2.2.1 Τομέας Power Train

Ο τομέας του «*Power Train*» αφορά στην κίνηση και τη μετάδοσης της. Μεταξύ άλλων είναι υπεύθυνο για τον κινητήρα, το κιβώτιο ταχυτήτων, το σύστημα μετάδοσης κίνησης και τα εξαρτήματα τους. Διαδραματίζει κρίσιμο ρόλο στον έλεγχο του κινητήρα και στη ρύθμιση διαφόρων παραμέτρων για την βελτίωση της οδηγικής εμπειρίας, της άνεσης, της κατανάλωσης καυσίμου και της μείωσης των εκπομπών καυσαερίων. Το σύστημα λαμβάνει πληροφορίες από πολλά συστήματα και λαμβάνει υπόψη παράγοντες όπως η θερμοκρασία του αέρα, το επίπεδο οξυγόνου και οι περιβαλλοντικές συνθήκες.

2.2.2.2 Τομέας Σασί

Το «*Chassis Domain*» κυρίως περιλαμβάνει συστήματα που ελέγχουν την αλληλεπίδραση του οχήματος με το δρόμο, όπως ο έλεγχος της πέδησης, των αναρτήσεων, της στρέψης των τροχών και του ελέγχου του οχήματος κτλ. Λαμβάνει υπόψη πληροφορίες προερχόμενες από πολλά διαφορετικά συστήματα και αφορούν τις επιλογές κίνησης, τις συνθήκες του δρόμου και τους περιβαλλοντικούς παράγοντες. Ιδιαίτερη έμφαση δίνεται στην ασφάλεια των ενσωματωμένων συστημάτων και τη διαδικασία αυθεντικοποίησης. Τεχνολογίες χρονικά πυροδοτούμενες, όπως το δίκτυο FlexRay, προσφέρουν κατάλληλες λύσεις παρά την περιορισμένη ευελιξία τους.

2.2.2.3 Τομέας Αμαξώματος

Ακολούθως ο τομέας του αμαξώματος («*Body Domain*») περιλαμβάνει λειτουργίες σχετικές με τον έλεγχο βοηθητικών εξαρτημάτων στο όχημα, όπως οι υαλοκαθαριστήρες, το απομακρυσμένο κλείδωμα και ξεκλείδωμα του οχήματος, οι καθρέπτες, τα παράθυρα κτλ. Δεν αναμένεται να διαδραματίσει κρίσιμο ρόλο για την ασφάλεια και την απόδοση του ευφυούς και συνδεδεμένου οχήματος, διότι αφορά δευτερεύοντες λειτουργίες που δεν επηρεάζουν την λειτουργικότητα, όμως η συμβολή τους είναι καθοριστική για την περίπτωση των μη αυτόνομων οχημάτων. Σε κάθε περίπτωση πρόκειται για έναν τομέα άμεσης διεπαφής του χρήστη με το όχημα, έτσι η αξιόπιστη και αποτελεσματική λειτουργία του θα παραμείνει υψηλά στην λίστα των κατασκευαστών.

2.2.2.4 Τομέας Αισθητήρων

Ένα από πιο κρίσιμα πεδία, για την ασφαλή κυκλοφορία, είναι αδιαμφισβήτητα αυτό των αισθητήρων. Κύριος σκοπός του «*Sensor Domain*» είναι η συλλογή δεδομένων σε πραγματικό χρόνο από το περιβάλλον του οχήματος. Περιλαμβάνει ένα ευρύ φάσμα αισθητήρων, όπως ραντάρ, Lidar, κάμερες και αισθητήρες υπερήχων, οι οποίοι επιτρέπουν στο όχημα να αντιλαμβάνεται το περιβάλλον του με ακρίβεια. Αυτοί οι αισθητήρες παρέχουν κρίσιμες πληροφορίες για προηγμένα συστήματα υποβοήθησης οδηγού (*Advanced Driver Assistance Systems)* και τεχνολογίες αυτόνομης οδήγησης, βοηθώντας το όχημα να λαμβάνει ενημερωμένες αποφάσεις και να αντιδρά κατάλληλα σε διάφορες οδικές συνθήκες.

2.2.2.5 Τομέας Τηλεματικής

Ο τομέας της τηλεματικής περιλαμβάνει την ενοποίηση των τηλεπικοινωνιών και της πληροφορικής στα οχήματα. Επιτρέπει την ανταλλαγή πληροφοριών μεταξύ του οχήματος και εξωτερικών συστημάτων, όπως υπηρεσίες που βασίζονται σε cloud, κέντρα διαχείρισης κυκλοφορίας και άλλα οχήματα. Η τηλεματική διευκολύνει λειτουργίες όπως απομακρυσμένα διαγνωστικά οχημάτων, υπηρεσίες πλοήγησης, βοήθεια έκτακτης ανάγκης, παρακολούθηση οχήματος και ενημερώσεις μέσω του αέρα. Αξιοποιώντας την τηλεματική, τα συνδεδεμένα οχήματα μπορούν να βελτιώσουν την ασφάλεια, να βελτιστοποιήσουν την απόδοση και να προσφέρουν μια σειρά εξατομικευμένων υπηρεσιών σε οδηγούς και επιβάτες.

2.2.2.6 Τομέας Πληροφόρησης και Διασκέδασης

Το έκτο πεδίο, ονομαζόμενο ως «*Infotainment Domain*» είναι αυτό με το οποίο αλληλεπιδρούν οι επιβάτες. Εστιάζει στην παροχή υπηρεσιών ψυχαγωγίας, συνδεσιμότητας και πληροφοριών. Περιλαμβάνει οθόνες αφής, συστήματα πολυμέσων, αναγνώριση φωνής, ενσωμάτωση έξυπνων τηλεφώνων, συνδεσιμότητα στο διαδίκτυο και εφαρμογές στο αυτοκίνητο, προσφέροντας ένα ευρύ φάσμα λειτουργιών, όπως ροή μουσικής, πλοήγηση, κλήσεις, ενσωμάτωση μέσων κοινωνικής δικτύωσης και πρόσβαση σε διάφορες διαδικτυακές υπηρεσίες, κάνοντας την εμπειρία οδήγησης πιο ευχάριστη και συνδεδεμένη. Επίσης προσφέρει στον επιβάτη πληροφορία για την κατάσταση του οχήματος, όπως η ταχύτητα, οι στροφές του κινητήρα, η πίεση των ελαστικών και του λαδιού κ.ά.

2.2.2.7 Τομέας Ενεργούς και Παθητικής Ασφαλείας

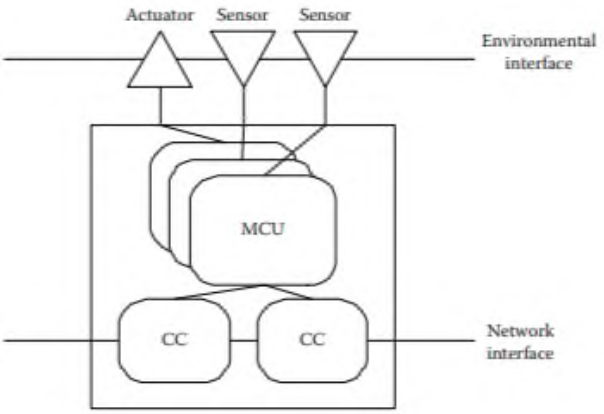
Τέλος, τα οχήματα είναι εξοπλισμένα με παθητικά τύπου μέτρα ασφαλείας, όπως οι ζώνες, οι αερόσακοι κτλ. τα οποία όμως έχουν φτάσει στα όρια τους ως προς την αποτελεσματικότητα τους στο να μειώνουν τους τραυματισμούς των επιβατών. Το γεγονός αυτό έχει προκαλέσει ήδη την στροφή σε ενεργητικού τύπου μέτρα, που θα στοχεύουν στην αποτροπή ενός ατυχήματος ή αν αυτό δεν μπορεί να αποφευχθεί στην μείωση της επίπτωσης τους στους επιβάτες και στο περιβάλλοντα χώρο. Τέτοια συστήματα είναι τα ABS, ESC, BASs κτλ. που ελέγχουν κρίσιμες λειτουργίες του οχήματος, όπως οι τροχοί, τα φρένα και πολλά άλλα.

2.2.3 Μονάδες Ηλεκτρονικού Ελέγχου

Καθένα από τα πεδία ηλεκτρονικών που εξετάστηκαν παραπάνω διαθέτει μια Ηλεκτρονική Μονάδα Ελέγχου (ΗΜΕ), γνωστή στη βιβλιογραφία ως ECU (Electronic Control Unit). Πρόκειται για μια υπολογιστική μονάδα υπεύθυνη για τον έλεγχο των λειτουργιών και υπηρεσιών του τομέα της (**Εικόνα 4**). Με απλά λόγια, αποτελεί τον εγκέφαλο του πεδίου, υπεύθυνο για την διαχείριση των πληροφοριών που φτάνουν σε αυτό από τα διάφορα στοιχεία και υποσυστήματα εντός του πεδίου ή των πληροφοριών που προέρχονται από άλλα πεδία.

Εικόνα 4 Παράδειγμα μιας ECU για το σύστημα EPS [1]

Ένα ECU ελέγχει ένα ή πολλαπλά συστήματα, συλλέγοντας δεδομένα, κάνοντας υπολογισμούς με αυτά και κατανέμοντας εντολές στα υπομέρη του συστήματος. Στο πυρήνα μια τέτοιας μονάδας (**Εικόνα 5**), βρίσκεται ένας μικροελεκτής (MCU: Microcontroller Unit), αποτελούμενος από μια κεντρική επεξεργαστική μονάδα, μνήμη και διεπαφές εισόδου/εξόδου. Προκειμένου να επικοινωνεί με τα στοιχεία του και το υπόλοιπα μέρη του οχήματος, διαθέτει κατάλληλους πομποδέκτες, που μπορούν να συνδυάζονται με μετατροπείς αναλογικού σε ψηφιακό (ADC) ή ψηφιακού σε αναλογικό (DAC) κτλ. Κάθε πεδίο μπορεί να διαθέτει παραπάνω από μια ΜΗΕ, για βοηθητικούς σκοπούς αναλόγως τις λειτουργίες και τις απαιτήσεις, όλες όμως τελικά απευθύνονται στην κύρια μονάδα ηλεκτρονικού ελέγχου του τομέα.



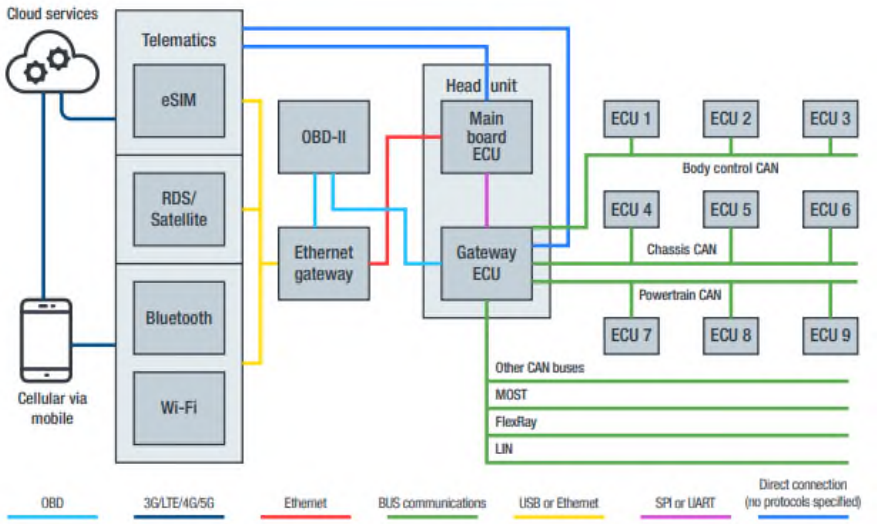
Εικόνα 5 Εσωτερική αρχιτεκτονικής μιας ECU [6]

2.3 Επικοινωνία

2.3.1 Δίκτυα Επικοινωνίας

Η εισαγωγή τεχνολογικά υψηλά ανεπτυγμένων ηλεκτρονικών και μικροελεγκτών, αφενός πρόσφεραν την δυνατότητα για πιο περίπλοκες υπηρεσίες και εφαρμογές αφετέρου όμως εισήγαγαν νέες απαιτήσεις στον τομέα των επικοινωνιών. Λόγω της κρισιμότητας αυτών των εφαρμογών, ο μηχανισμός της επικοινωνίας πρέπει να φέρει εγγυήσεις αξιοπιστίας, απόδοσης, ευελιξίας αλλά και χαμηλού κόστους. Ένα ευφυές και συνδεδεμένο όχημα υποστηρίζει δύο είδη επικοινωνίας, έναν μηχανισμό αλληλεπίδρασης με το εξωτερικό του περιβάλλον (**Εικόνα 6**) και ένα για τον συντονισμό των εσωτερικών του τμημάτων και στοιχείων (**Εικόνα 7**).

Εικόνα 6 Αναπαράσταση εξωτερικού δικτύου επικοινωνίας ενός ICV [20]



Εικόνα 7 Αναπαράσταση εσωτερικού δικτύου επικοινωνίας ενός ICV [30]

Η αρχιτεκτονική της ενδοεπικοινωνίας προκειμένου να καλύψει τις αυξημένες απαιτήσεις, υποστηρίζει απευθείας σύνδεση των ECU μέσα από κοινά μέσα επικοινωνίας, εξασφαλίζοντας συγχρονισμό και αξιόπιστη ανταλλαγή δεδομένων. Έχουν σχεδιαστεί και υλοποιηθεί πολλές διαφορετικές τοπολογίες δικτύων - σημείο-προς-σημείο, αστέρα, υβριδικά - όπως επίσης και αρκετοί τύποι καλωδίων, διαύλων επικοινωνίας, καθένας με τα δικά του χαρακτηριστικά ως προς την ταχύτητα, την αξιοπιστία, το κόστος κτλ. Η ακριβής τοπολογία και ο δίαυλος με την οποία συνδέονται μονάδες ηλεκτρονικού ελέγχου, έχουν άμεση εξάρτηση από το πρωτόκολλο επικοινωνίας που έχει επιλεγεί για να υποστηρίξει το συγκεκριμένο σύστημα του οχήματος.

2.3.2 Επισκόπηση Πρωτοκόλλων Επικοινωνίας

Τα σύγχρονα αυτοκίνητα λειτουργούν σε αντίξοα περιβάλλοντα και έχουν υψηλές απαιτήσεις και αυστηρές προδιαγραφές. Κατά συνέπεια έχει δημιουργηθεί η ανάγκη για αυξημένες ταχύτητες μεταδόσεων πληροφοριών, ισχυρές πιστοποιήσεις ασφαλείας αλλά και ντετερμινιστική κυκλοφορία δεδομένων. Μια τεχνολογία που μπορεί να εξυπηρετήσει τις ανάγκες αυτές είναι τα χρονο-πυροδοτούμενα, time-triggered, πρωτόκολλα επικοινωνίας. Τα τελευταία χρόνια έχουν αναπτυχθεί πολλά ενσωματωμένα δίκτυα αυτοκινήτων, όπως το τοπικό δίκτυο διασύνδεσης γνωστό ως LIN, το CAN, το FlexRay και το MOST. Οι διαφορετικές ιδιότητες και τα χαρακτηριστικά καθενός από αυτά οδήγησε στην ιδέα της πολυπλεξίας (**Εικόνα 8**), δηλαδή της χρήσης

πολλών από αυτών σε διαφορετικά τμήματα και υποσυστήματα του ίδιου αυτοκινήτου, προκαλώντας τη σημαντική μείωση του κόστους καλωδίωσης καθώς και τη παροχή αυξημένης ευελιξίας στους σχεδιαστές, αφού τα δεδομένα που δειγματοληπτούνται από έναν μικροελεγκτή γίνονται διαθέσιμα σε απομακρυσμένες λειτουργίες που τις χρειάζονται χωρίς πρόσθετους αισθητήρες. Οι δίαυλοι επικοινωνίας διακρίνονται σε τέσσερεις κλάσεις A, B, C και D ανάλογα με τα χαρακτηριστικά του πρωτόκολλου.

Category	Bus Name	Communication Rate	Application
A	LIN	Below 10 kbps	Headlights, lights, door locks, power seats, etc.
B	CAN	10 kbps to 125 kbps	Automotive air conditioning, electronic instructions, fault detection, etc.
C	FlexRay	125 kbps to 1 Mbps	Engine control, steering-by-wire system, anti-lock braking system, suspension control, etc.
D	MOST/1394	More than 2 Mbps	Multimedia entertainment system, car navigation system, etc.

Εικόνα 8 Επισκόπηση πρωτοκόλλων επικοινωνίας [5]

2.3.2.1 Controlled Area Network (CAN)

Το πιο διαδεδομένο πρωτόκολλο για εφαρμογές τέτοιου τύπου, το CAN, αποτελεί ακόμα μια από τις πρώτες επιλογές των κατασκευαστών. Με δίαυλο κλάσης B, υποστηρίζει μεταδόσεις μεταξύ κόμβων και είναι φθηνό, γρήγορο (1Mb/s), ασφαλές, αξιόπιστο σε δυσμενείς συνθήκες και οδήγησε στην μείωση του απαιτούμενου καλωδίου στο όχημα. Πρόκειται για ένα event-triggered πρωτόκολλο, δηλαδή πυροδοτούμενο από γεγονότα, βασισμένο σε multi-master λογική. Κάθε μήνυμα σε ένα cluster μεταδίδεται μόνο όταν υπάρχει ανάγκη και γίνεται broadcast σ' όλους τους κόμβους αυτού. Το αναγνωριστικό ενός μηνύματος αφορά αποκλειστικά στα περιεχόμενα του και όχι στην πηγή προέλευσης. Ταυτόχρονα, το αναγνωριστικό δηλώνει προτεραιότητα. Όταν εντοπίζεται μια σύγκρουση, το πακέτο που κυριαρχεί είναι αυτό με την υψηλότερη προτεραιότητα, δηλαδή το μικρότερο αναγνωριστικό.

2.3.2.2 Local Interconnect Network (LIN)

Πιο φθηνό και λιγότερο αποδοτικό (20kb/s) από το CAN, χρησιμοποιείται κυρίως σε βοηθητικές λειτουργίες και συστήματα, που δεν κρίνονται τόσο κρίσιμα για την συνολική λειτουργία του οχήματος, όπως για παράδειγμα ο έλεγχος των παραθύρων. Ακολουθεί πολιτική single master-multiple slaves με τον master να εκκινεί τις

μεταδόσεις και η επιλογή του εισάγει έμμεσα, ένα έξτρα επίπεδο ασφαλείας, αφού μια δυσλειτουργία σε ένα λιγότερο κρίσιμο σύστημα δεν θα επηρεάσει τα πιο κρίσιμα συστήματα που τρέχουν με FlexRay ή CAN. Ο δίαυλος που χρησιμοποιείται είναι κλάσης Α, δηλαδή πολλαπλό σύστημα καλωδίων που επιτρέπει την μείωση των απαιτήσεων σε καλώδιο μέσω της γενικής σκοπού ασύγχρονης μετάδοσης και λήψης (Universal Purpose Asynchronous, UART) που υποστηρίζει, με πολλαπλά σήματα πάνω στο ίδιο μοναδικό κανάλι.

2.3.2.3 Media Oriented System Transport (MOST)

Όπως υποδεικνύει και το όνομα, χρησιμοποιήθηκε προκειμένου να αντικαταστήσει τα παλιά πρωτόκολλα που χρησιμοποιούνταν σε ενσωματωμένες συνδέσεις ήχου. Κύριος σκοπός του η εγκαθίδρυση επικοινωνίας ανάμεσα σε μονάδες και συστήματα που αφορούν λειτουργίες εγγενείς στους επιβάτες. Στα πλεονεκτήματα του, παρέχει φυσικό επίπεδο για την υλοποίηση του ethernet σε ενσωματωμένες επικοινωνίες. Ο δίαυλος του χαρακτηρίζεται κλάσης D, υποστηρίζοντας υψηλής απόδοσης δίκτυα και υψηλές ταχύτητες μεταδόσεων ροών δεδομένων.

2.3.2.4 X-by-Wire

Ο όρος αυτός, επινοήθηκε προκειμένου να συμβολίσει τις εφαρμογές που ελέγχονται από ηλεκτρικές συνδέσεις καλωδίων. Κατάλληλα για υψηλής κρισιμότητα συστήματα, εξασφαλίζει ασφάλεια των δεδομένων και ανοχή σφαλμάτων σε συνθήκες υψηλών ταχυτήτων λειτουργίας. Όσο η πολυπλοκότητα, οι υπολογιστικές ανάγκες και οι απαιτήσει των δικτύων επικοινωνίας αυξάνουν τόσο τα πρωτόκολλα αυτά κερδίζουν έδαφος. Με καλώδιο τύπου C, μεταφέρει μεγάλο πλήθος δεδομένων με σήματα πραγματικού χρόνου. Σχεδιασμένα για να επιλύουν το πρόβλημα της έλλειψης ντετερμινισμού στα δεδομένα, επινοήθηκαν διάφορα πρωτόκολλα x-by-wire, όπως τα CAN-FD, TTCAN, TTP/C, Byteflight και FlexRay, με το τελευταίο να κερδίζει την δημοτικότητα.

2.4 Κίνδυνοι

Με την διαρκώς αυξανόμενη ψηφιοποιήση των αυτοκινήτων εντείνονται οι ανησυχίες για κακόβουλες ενέργειες που θα οδηγήσουν σε απώλειες ζωών, ατυχήματα ή οικονομικές ζημίες. Η δυνατότητα των οχημάτων να συνδέονται και να

επικοινωνούν με αντικείμενα στο περιβάλλον, διευρύνει το διαθέσιμο εύρος επιλογών για έναν επιτιθέμενο. Δύναται να έχει πρόσβαση σε προσωπικές πληροφορίες όπως η μουσική που ακούν οι επιβάτες, κλήσεις και συνομιλίες αυτών, το στίγμα του GPS τους ή σε κρίσιμες για την ασφάλεια και την λειτουργικότητα όπως τον έλεγχο των φρένων, των αισθητήρων κτλ. Κατά συνέπεια η ανάπτυξη έξυπνων και συνδεδεμένων οχημάτων δεν είναι χωρίς προκλήσεις. Η διασφάλιση ισχυρών μέτρων κυβερνοασφάλειας, η αντιμετώπιση των ανησυχιών περί απορρήτου και η δημιουργία αξιόπιστης υποδομής επικοινωνίας είναι μεταξύ των βασικών εμποδίων που πρέπει να ξεπεραστούν για ευρεία υιοθέτηση.

2.4.1 Αρχές Ασφαλείας

Πολύ σημαντικό για τους μηχανικούς ασφαλείας είναι κατατοπισμένοι για το βασικό σχήμα των αρχών ασφαλείας που πρέπει να ακολουθούνται για την αποφυγή και την καταστολή των επιθέσεων. Όπως και σε άλλες εφαρμογές, έτσι και στα ευφυή και συνδεδεμένα οχήματα αυτές περιγράφονται από το Parkerian Hexad που εισάγει τρείς επιπλέον αρχές από αυτές του CIA Triad [4] και το οποίο φαίνεται στην παρακάτω εικόνα (**Εικόνα 9**).

Εικόνα 9 Αρχές ασφαλείας έναντι επιθέσεων [4]

2.4.1.1 Εμπιστευτικότητα

Η εμπιστευτικότητα διασφαλίζει πως οι ευαίσθητες πληροφορίες είναι προστατευμένες από μη εξουσιοδοτημένη πρόσβαση. Περιλαμβάνει μηχανισμούς κρυπτογράφησης, ελέγχου της πρόσβασης και αποφυγής διαρροής δεδομένων στα κανάλια επικοινωνίας.

2.4.1.2 Ακεραιότητα

Η ακεραιότητα αφορά στην ακρίβεια, στη συνέπεια και στην αξιοπιστία των δεδομένων και των συστημάτων. Περιλαμβάνει την αποτροπή μη εξουσιοδοτημένης τροποποίησης, αλλαγής ή καταστροφής δεδομένων και τη διασφάλιση ότι τα δεδομένα παραμένουν άθικτα και άθικτα καθ' όλη τη διάρκεια του κύκλου ζωής τους.

2.4.1.3 Διαθεσιμότητα

Η διαθεσιμότητα διασφαλίζει ότι τα συστήματα και οι πόροι είναι προσβάσιμα όταν χρειάζεται. Περιλαμβάνει την εφαρμογή μέτρων για την πρόληψη και τον μετριασμό των διακοπών, όπως αστοχίες υλικού ή λογισμικού, διακοπές δικτύου ή επιθέσεις άρνησης υπηρεσίας (DoS), που θα μπορούσαν να οδηγήσουν σε μη διαθεσιμότητα υπηρεσιών.

2.4.1.4 Αυθεντικότητα

Η αυθεντικότητα επαληθεύει την ταυτότητα και την προέλευση οντοτήτων, όπως χρήστες, συστήματα ή πηγές δεδομένων. Περιλαμβάνει την εφαρμογή μηχανισμών για τον έλεγχο ταυτότητας και τη μη απόρριψη, διασφαλίζοντας ότι οι οντότητες μπορούν να είναι αξιόπιστες και οι ενέργειές τους μπορούν να αποδοθούν αξιόπιστα.

2.4.1.5 Κατοχή ή Έλεγχος

Ο έλεγχος αναφέρεται στη θέσπιση και επιβολή κατάλληλων πολιτικών, διαδικασιών και διασφαλίσεων ασφαλείας. Περιλαμβάνει την εφαρμογή ελέγχων πρόσβασης, σχέδια αντιμετώπισης συμβάντων και άλλα μέτρα για τον μετριασμό των κινδύνων και τη διατήρηση ενός ασφαλούς περιβάλλοντος.

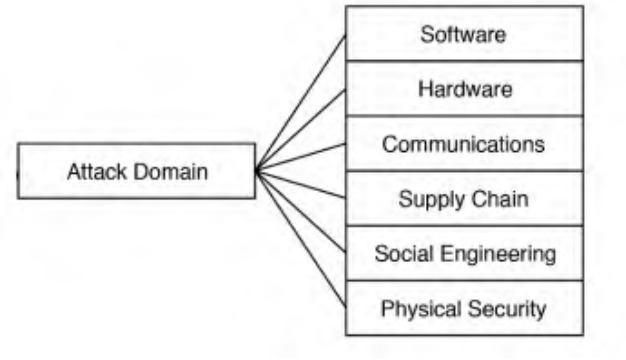
2.4.1.6 Χρησιμότητα

Η χρησιμότητα αναφέρεται στην αρχή της εξισορρόπησης των μέτρων ασφαλείας με τη χρηστικότητα και τη λειτουργικότητα των συστημάτων. Περιλαμβάνει την εύρεση της σωστής ισορροπίας μεταξύ των απαιτήσεων ασφαλείας και της εμπειρίας του χρήστη για να διασφαλιστεί ότι τα μέτρα ασφαλείας δεν εμποδίζουν την προβλεπόμενη λειτουργικότητα ή χρηστικότητα των συστημάτων.

2.4.3 Μοντέλα Απειλής

Πρώτο βήμα ενός μηχανικού που ασχολείται με την κυβερνοασφάλεια είναι η μελέτη των μηχανισμών και των μοντέλων απειλής (**Εικόνα 10**) του υπό μελέτη συστήματος.

Το βήμα αυτό είναι από τα πιο κρίσιμα αφού δίνει πληροφόρηση για τα σημεία από τα οποία μπορεί να υπάρξει πρόσβαση στο σύστημα και να εφαρμοστούν επιθέσεις.



Εικόνα 10 Μοντέλα απειλής [3]

Η συγκέντρωση και η δημοσιοποίηση των διανυσμάτων είναι πολύ σημαντική, όμως λόγω της πολύ πρόσφατης ανάδειξης των κινδύνων στα ευφυή και συνδεδεμένα οχήματα, η βιβλιογραφία είναι περιορισμένη. Έχουν γίνει αρκετές προσπάθειες ταξινόμησης των μηχανισμών με διαφορετικά κριτήρια η κάθε μια. Στα πλαίσια της διπλωματικής μελετήθηκαν αρκετές πηγές και παρακάτω παρουσιάζεται μια όσο το δυνατόν πιο ολοκληρωμένη ταξινόμηση βάσει του πεδίου εφαρμογής αυτής.

2.4.3.1 Επιθέσεις Λογισμικού

Στοχεύουν στην ανάδειξη ευπαθειών στο λειτουργικό σύστημα του οχήματος, στο υλικολογισμικό ή σε εφαρμογές που μπορεί να εκτελούνται σε αυτό. Οι ακριβείς μηχανισμοί ποικίλουν από απομακρυσμένες εκτελέσεις κώδικα μέχρι έγχυση κακόβουλου κώδικα ή χειραγώγηση των ενημερώσεων του λογισμικού.

2.4.3.2 Επιθέσεις Υλικού

Πρόκειται για επιθέσεις στις μονάδες υλικού με στόχο την χειραγώγηση συγκεκριμένων τμημάτων. Αφορά τις ECU, τους αισθητήρες και άλλους ελεγκτές ή τμήματα υλικού, στα οποία πραγματοποιείται μη αυθεντικοποιημένη πρόσβαση και διακόπτεται ή τροποποιείται η λειτουργικότητα τους.

2.4.3.3 Επιθέσεις Επικοινωνίας

Αφορούν στην ανάδειξη ευπαθειών στα δίκτυα επικοινωνίας του οχήματος είτε ενσύρματα είτε ασύρματα. Περιλαμβάνουν μη εξουσιοδοτημένες προσβάσεις σε

δεδομένα, παρακολούθηση και συλλογή πακέτων ή ακόμα και παρεμβολή στην επικοινωνία μέσω της αποστολή ή τροποποίησης μηνυμάτων.

2.4.3.4 Επιθέσεις Αλυσίδας Τροφοδοσίας

Στην περίπτωση αυτή η κακόβουλη ενέργεια βρίσκει εφαρμογή στην βιομηχανική επεξεργασία των τμημάτων ή στην διαδικασία μεταφοράς τους. Συνήθως περιλαμβάνουν την εισαγωγή επιπλέον κυκλωματικής λογικής στο υλικό, όπως τα hardware trojans ή στην πρόκληση συγκεκριμένης ζημίας, με απώτερο στόχο την προσθήκη ή αφαίρεση αντίστοιχα κάποιας λειτουργικότητας ή την δημιουργία μιας ευπάθειας.

2.4.3.5 Επιθέσεις Κοινωνικής Μηχανικής

Οι επιθέσεις κοινωνικής μηχανικής στοχεύουν τους ανθρώπους προκειμένου να επέλθει πρόσβαση στο όχημα. Συνήθως εφαρμόζεται μέσω της ψηφιακής εξαπάτησης τους, με απώτερο στόχο την παροχή στον επιτιθέμενο άδειας πρόσβασης σε ευαίσθητες πληροφορίες ή την συλλογή αυτών.

2.4.3.6 Επιθέσεις Φυσικής Ασφάλειας

Όπως προϊδεάζει και το όνομα, αφορά σε επιθέσεις που στοχεύουν απευθείας μέσω της φυσικής πρόσβασης στο όχημα. Συνήθως συνδυάζεται με παράνομη παραβίαση του οχήματος προκειμένου να παρακαμφθούν οι μηχανισμοί κλειδώματος και συναγερμού αυτού.

Κεφάλαιο 3 Πρωτόκολλο FlexRay

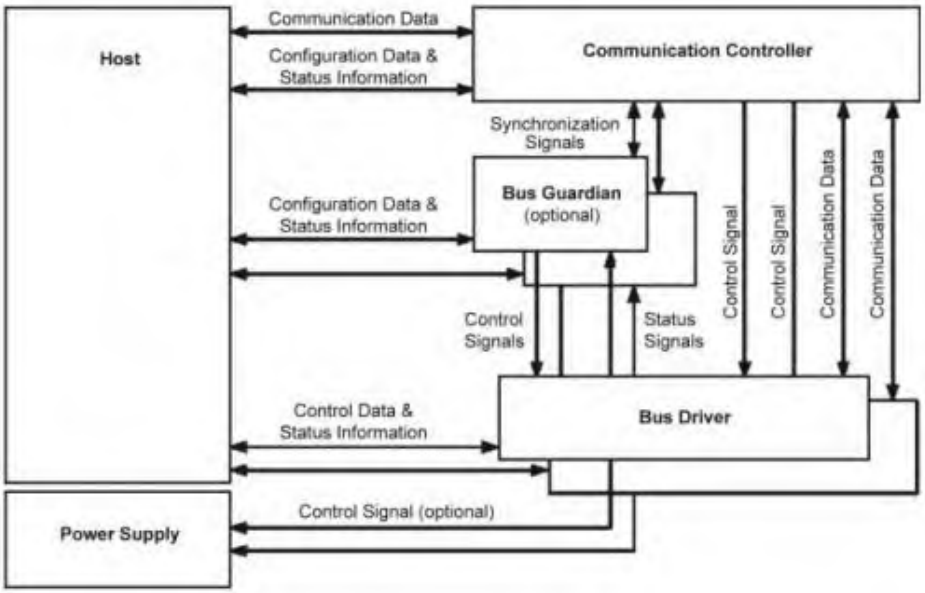
3.1 Εισαγωγή

Το FlexRay είναι το πιο διαδεδομένο X-by-wire πρωτόκολλο, διότι προσφέρει υψηλή ταχύτητα, ανοχή σε σφάλματα, ντετερμινιστικότητα και είναι πυροδοτούμενο τόσο από το χρόνο (time triggered) όσο και γεγονότα (event triggered). Η πολιτική που ακολουθεί είναι αυτή ενός multi-master πρωτοκόλλου, όπου η πρόσβαση στο δίαυλο είναι αυστηρά καθορισμένη και βασισμένη σε κύκλους επικοινωνίας. Στηρίζεται σε σχήμα πολλαπλής πρόσβασης σε διαιρεμένο χρόνο (Time-Division Multiple Access, TDMA), όπου κάθε πλαίσιο δεσμεύεται για μετάδοση σε συγκεκριμένη χρονοθυρίδα. Έτσι εξασφαλίζεται ο ντετερμινισμός των δεδομένων αφού κάθε πλαίσιο μεταδίδεται σε συγκεκριμένες χρονικές μονάδες, σε προκαθορισμένο χρόνο και κύκλους επικοινωνίας. Σχεδιασμένο με δύο διαύλους δύναται να αξιοποιεί και τους δύο, αναλόγως τις απαιτήσεις σε ανοχή σφαλμάτων και επιπρόσθετο bandwidth. Για να λειτουργήσει σωστά θα πρέπει οι παράμετροι του δικτύου να είναι γνωστές σε όλους τους κόμβους που συμμετέχουν σε αυτό.

3.2 Αρχιτεκτονική

3.2.1 Κόμβος

Ένας FlexRay κόμβος, είναι στην πραγματικότητα ένα ECU. Τα κύρια μέρη του, όπως φαίνεται στην παρακάτω εικόνα (**Εικόνα 11**), είναι ο host microcontroller, ο protocol manager, ο line driver και προαιρετικός bus guardian που εξασφαλίζει την σωστή πρόσβαση στο μέσο.



Εικόνα 11 Βασική αρχιτεκτονική ενός FlexRay κόμβου [1]

Σε κάθε στιγμή μπορεί να παίζει έναν από τους παρακάτω ρόλους:

1. Συγχρονισμός: ένας κόμβος συγχρονισμού (sync node) συμμετέχει σε έναν αλγόριθμο συγχρονισμού του cluster, κατά την διάρκεια του οποίου μεταδίδονται πλαίσια συγχρονισμού (sync frame), τα οποία λαμβάνονται από όλους τους κόμβους. Σκοπός της διαδικασίας αυτής, είναι ο συγχρονισμός των clock rate, και άρα ο προσδιορισμός των cycle length και clock offset και άρα του σημείου εκκίνησης του κύκλου.
2. Cold Start: είναι οι κόμβοι που αρχικοποιούν μια επικοινωνία. Μπορούν να μεταδώσουν πλαίσια εκκίνησης (startup frames), δηλαδή πλαίσια που εγκαθιδρύουν και εκκινούν μια επικοινωνία. Ένα coldstart node είναι πάντα sync node και το αντίστροφο.
3. Non-Sync Node: όταν δεν έχει να επιτελέσει κάποια από τις προαναφερθείσες λειτουργίες.

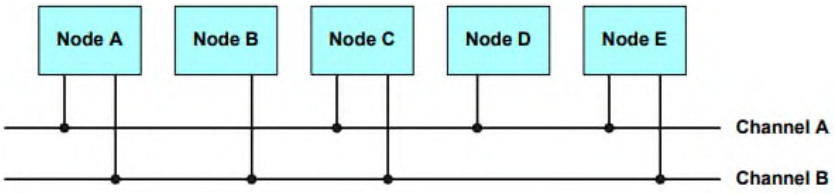
3.2.2 Δίκτυο

Ένα δίκτυο FlexRay αποτελείται το πολύ μέχρι δύο διαύλους επικοινωνίας, το κανάλι Α και το κανάλι Β. Κάθε κόμβος συνδέεται είτε στο ένα είτε και στα δύο, και στη κατάσταση ελεύθερη από σφάλματα (fault free) επικοινωνεί μόνο με τους κόμβους που βρίσκονται συνδεδεμένοι επίσης στο ίδιο κανάλι με αυτόν. Αν ένας κόμβος

πρέπει να ανήκει σε περισσότερα από ένα clusters τότε πρέπει να χρησιμοποιείται διαφορετικός ελεγκτής δικτύου. Ακολουθούν οι τοπολογίες του FlexRay πρωτοκόλλου.

3.2.2.1 Passive Bus Topology

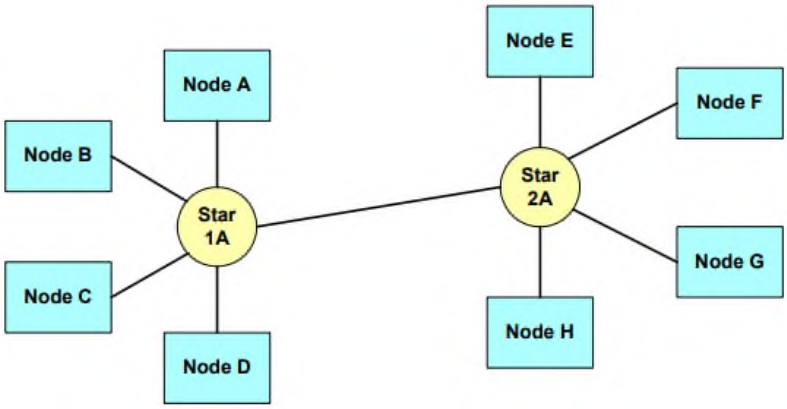
Όλες οι ECU συνδέονται σε ένα καλώδιο με διακλαδώσεις για καθένα από αυτούς (**Εικόνα 12**).



Εικόνα 12 Παθητική τοπολογία διαύλου FlexRay [2]

3.2.2.2 Active Star Topology

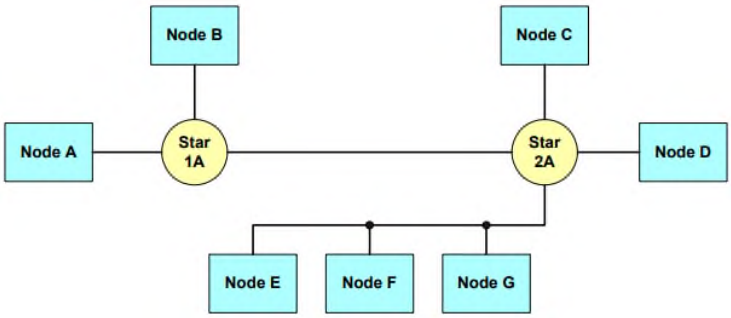
Το δίκτυο FlexRay μπορεί να σχεδιαστεί ως τοπολογία πολλαπλών αστέρων (**Εικόνα 13**). Οι ECU συνδέονται σε έναν κεντρικό κόμβο προσφέροντας περισσότερες εγγυήσεις αξιοπιστίας, αφού ακόμα και αν δυσλειτουργεί μια ECU οι υπόλοιπες δεν θα επηρεαστούν. Η συγκεκριμένη τοπολογία επίσης επιτρέπει την αποφυγή σημείων που μπορούν να δημιουργήσουν παρεμβολές στο καλώδιο.



Εικόνα 13 Ενεργή τοπολογία διαύλου FlexRay [2]

3.2.2.3 Hybrid Bus Topology

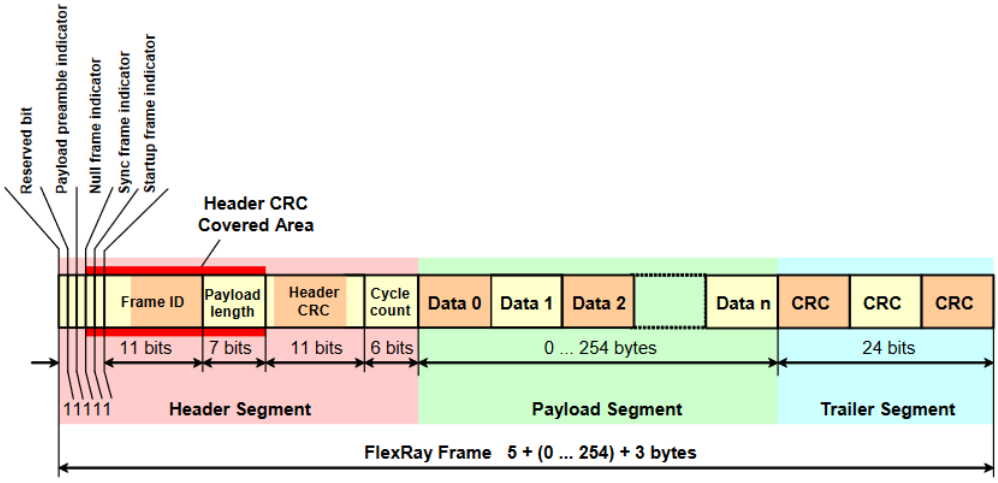
Πρόκειται για τον συνδυασμό των δύο παραπάνω τοπολογιών (**Εικόνα 14**) για την επίτευξη της καλύτερης λύσης αναλόγως την περίπτωση. Σχηματίζεται και κατά την σύνδεση επιμέρους διαφορετικών τοπολογιών.



Εικόνα 14 Υβριδική τοπολογία διαύλου FlexRay [2]

3.3 Μορφή Πλαισίου

Το FlexRay πλαίσιο, χωρίζεται σε τρία κύρια τμήματα, αυτό της κεφαλής (header segment), αυτό των δεδομένων (payload segment) και αυτό της ουράς (trailer segment). Κάθε τμήμα διακρίνεται σε πεδία με συγκεκριμένο μέγεθος, όπως φαίνεται στην παρακάτω εικόνα (**Εικόνα 15**).



Εικόνα 15 Μορφή ενός FlexRay πλαισίου [2]

3.3.1 Τμήμα Κεφαλής

Έχει μέγεθος 5 Bytes και περιέχει τα εξής πεδία:

- **Reserved Bit (1 bit)**: το πεδίο αυτό προς το παρόν, δεν παίζει κάποιο ρόλο αλλά υπάρχει για μελλοντική χρήση. Ο αποστολέας πρέπει να το θέτει σε μηδέν και ο παραλήπτης να το αγνοεί.
- **Payload Preamble Indicator (1 bit)**: η τιμή του δείχνει αν υπάρχει μια προαιρετική πληροφορία στο τμήμα των δεδομένων. Στο στατικό τμήμα, κατά την διάρκεια ενός κύκλου, η πληροφορία αυτή ονομάζεται Network

Management Vector ενώ στο δυναμικό τμήμα Message Indicator. Ο σκοπός και η μορφή αυτής της πληροφορίας θα αναλυθεί παρακάτω.

- **Null Frame Indicator (1 bit)**: καθορίζει αν πρόκειται για null frame, δηλαδή για πλαίσιο που δεν φέρει χρήσιμη πληροφορία στο τμήμα των δεδομένων. Αν η τιμή είναι μηδέν, τότε το τμήμα των δεδομένων είναι μηδενικό και άκυρο. Αν η τιμή είναι 1 τότε περιέχει χρήσιμα δεδομένα.
- **Sync Frame Indicator (1 bit)**: Αν είναι 0 τότε κανένας κόμβος-παραλήπτης δεν πρέπει να λάβει υπόψιν το πλαίσιο για διαδικασίες συγχρονισμού. Αντίθετα η τιμή 1 σημαίνει πως όλοι οι κόμβοι πρέπει να το χρησιμοποιήσουν για τον συγχρονισμό των ρολογιών τους.
- **Startup Frame Indicator (1 bit)**: Μόνο οι coldstart κόμβοι μπορούν να μεταδώσουν ένα πλαίσιο με τιμή του δείκτη αυτού ίσο με 1, δηλαδή ένα startup frame.
- **Frame Indicator (11 bits)**: Καθορίζει τη χρονοθυρίδα στην οποία το πλαίσιο πρέπει να μεταδοθεί και δεν πρέπει να χρησιμοποιείται περισσότερες φορές από μια στην διάρκεια ενός κύκλου επικοινωνίας. Κάθε πλαίσιο εντός ενός cluster έχει ένα αναγνωριστικό πλαισίου και οι τιμές που μπορεί αυτό να λάβει είναι από 1 έως 2047, όχι την τιμή 0.
- **Payload Length (7 bits)**: φέρει πληροφορία για το μέγεθος του τμήματος, των δεδομένων. Η τιμή αυτή δεν ενημερώνει για το συνολικό μέγεθος σε Bytes αλλά για το μισό αυτού. Κατά την διάρκεια του στατικού τμήματος, το μέγεθος είναι σταθερό για όλα τα πλαίσια και ίσο με 127, δηλαδή 254 Bytes. Αντίθετα στο δυναμικό τμήμα, μπορεί να διαφέρει μεταξύ διαφορετικών πλαισίων του ίδιου κύκλου, διαφορετικών κύκλων ή διαφορετικών καναλιών.
- **Header CRC (11 bits)**: περιέχει το cyclic redundancy check code (CRC) υπολογισμένο πάνω στα πεδία sync frame indicator, startup frame indicator, frame indicator και το payload length. Το πολυώνυμο του αλγορίθμου είναι

$$x^{11} + x^9 + x^8 + x^7 + x^2 + 1 = 0x385$$

και ο καταχωρητής αρχικοποιείται στην τιμή 0x01A.

- **Cycle Count (6 bits)**: υποδεικνύει την τιμή του μετρητή κύκλου από την πλευρά του κόμβου μετάδοσης, την στιγμή της μετάδοσης.

3.3.2 Τμήμα Δεδομένων

Το τμήμα αυτό έχει μέγεθος από 0 έως 254 Bytes και απαριθμούνται ως Data 0, Data 1 κτλ. Το πεδίο payload preamble indicator που βρίσκεται το τμήμα κεφαλής, καθορίζει αν στα πρώτα Byte αυτού του πεδίου περιέχεται μια επιπλέον προαιρετική πληροφορία, μη σχετική με τα δεδομένα. Αυτή μπορεί να είναι είτε το διάνυσμα διαχείρισης του δικτύου (Network Management Vector) είτε το αναγνωριστικό μηνύματος (Message ID). Το πρώτο αφορά στο στατικό τμήμα του κύκλου και περιέχει πληροφορία που έχει συλλέξει ο ελεγκτής επικοινωνίας κατά την διάρκεια των χρονοθυρίδων. Το δεύτερο εντοπίζεται στο δυναμικό τμήμα και φέρει μια συμπληρωματική πληροφορία στην αρχή του τμήματος δεδομένων που χρησιμοποιείται στη διάκριση των περιεχομένων του πλαισίου.

3.3.3 Τμήμα Ουράς

Αποτελούμενο από τρία πεδία των 24 bit, έχει ως στόχο την υποστήριξη της ανίχνευσης σφαλμάτων κατά την διάρκεια μετάδοσης ή αποθήκευσης δεδομένων, με την χρήση του Κυκλικού Ελέγχου Πλεονασμού (Cyclic Redundancy Check, CRC). Το πολυώνυμο που χρησιμοποιείται είναι το

$$x^{24} + x^{22} + x^{20} + x^{19} + x^{18} + x^{16} + x^{14} + x^{13} + x^{11} + x^{10} + x^{8} + x^{7} + x^{6} + x^{3} + x + 1 = 0x5D6DCB$$

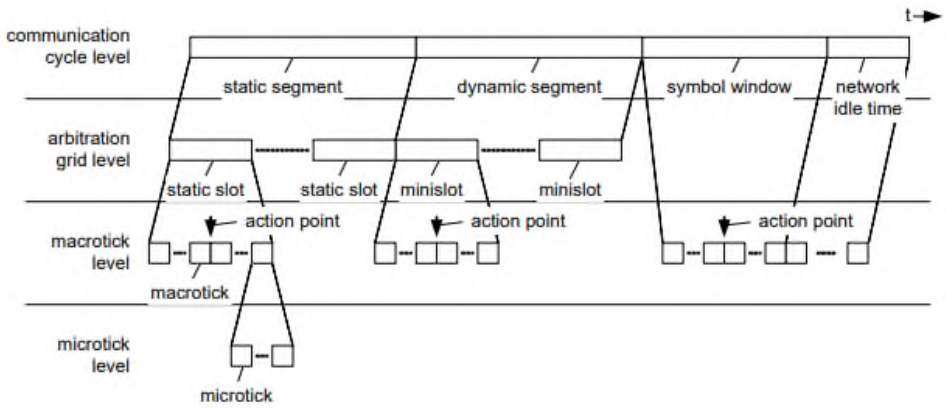
και ο καταχωρητής αρχικοποιείται αναλόγως το κανάλι. Στην περίπτωση του καναλιού B με την τιμή 0XABCDEF και του καναλιού A με την τιμή 0XFEDCBA. Ο αλγόριθμος υπολογίζεται πάνω και στα δύο κανάλια και έξω από τον Ελεγκτή Επικοινωνίας (Communication Controller, CC).

3.4 Κύκλος Επικοινωνίας

3.4.1 Δομή

Όπως αναφέρθηκε στην εισαγωγή (**3.1 Εισαγωγή**) το FlexRay στηρίζεται σε ένα σχήμα πολλαπλής πρόσβασης σε διαιρεμένο χρόνο. Αυτό σημαίνει πως όλοι οι συμμετέχοντες κόμβοι εντός ενός δικτύου μεταδίδουν τα μηνύματα τους στην ίδια συχνότητα αλλά σε διαφορετικές χρονικές περιόδους. Το χρονικό φάσμα διαιρείται σε χρονοθυρίδες (time slots), οι οποίες μοιράζονται στους κόμβους. Όταν μια χρονοθυρίδα ανήκει σε έναν κόμβο τότε μόνο αυτός μπορεί να μεταδώσει δεδομένα.

Σε κάθε άλλη χρονοθυρίδα παρακολουθεί το κανάλι για δεδομένα από άλλους κόμβους. Το σχήμα αυτό επαναλαμβάνεται κυκλικά τόσες φορές όσοι οι κύκλοι επικοινωνίας που καθορίστηκαν κατά την διαδικασία startup. Κατά συνέπεια οι συμμετέχοντες στο δίκτυο θα πρέπει να περιμένουν την κατάλληλη χρονική στιγμή, η οποία τους έχει ανατεθεί προκειμένου να στείλουν δεδομένα και άρα τα μηνύματα τα οποία παράγονται εκτός της δεσμευμένης χρονοθυρίδας θα πρέπει να αποθηκεύονται μέχρι την επόμενη (Buffer and Burst). Θεμελιώδη αρχή στο σχήμα αυτό αποτελεί ο κύκλος επικοινωνίας που διακρίνεται σε χρονικά επίπεδα ιεραρχίας (**Εικόνα 16**).

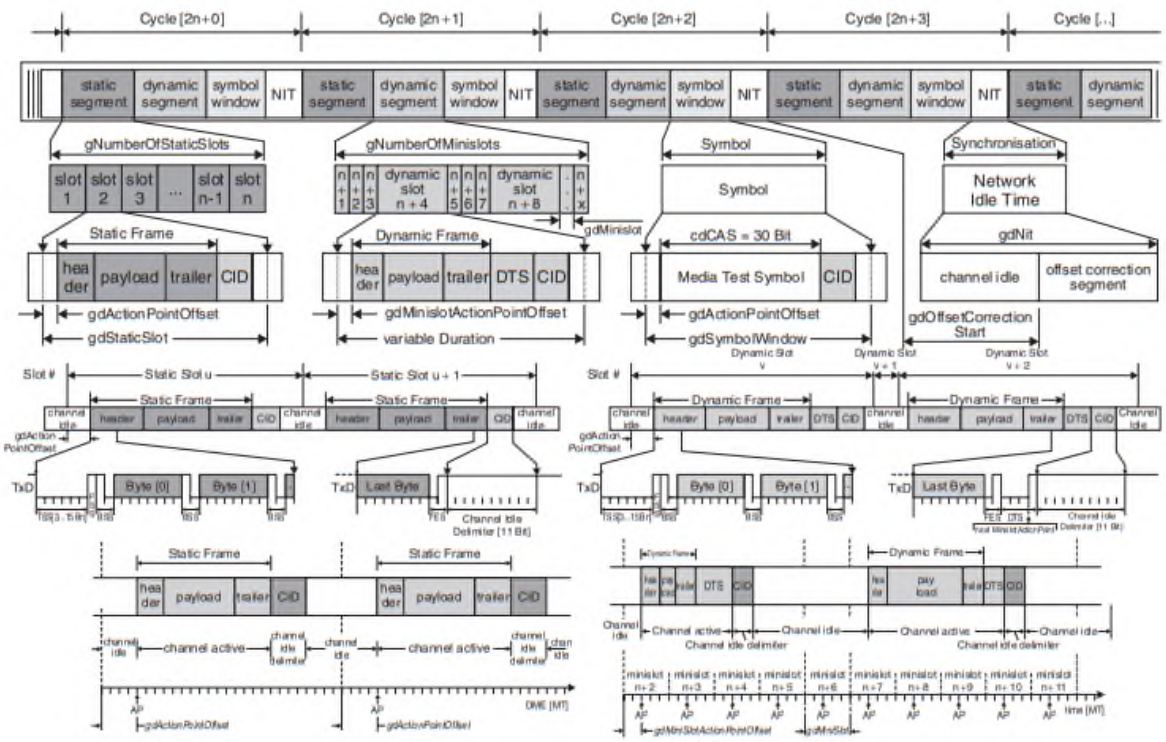


Εικόνα 16 Δομή κύκλου επικοινωνίας FlexRay [2]

Όπως φαίνεται από την εικόνα, οι χρονοθυρίδες και οι μίνι-θυρίδες χωρίζονται σε μικρότερες υπομονάδες χρόνου. Μεταξύ των κόμβων η μικρότερη μονάδα είναι αυτή του macrotick. Όλα τα μέρη ενός δικτύου συγχρονίζουν και ρυθμίζουν τα ρολόγια τους ώστε να δημιουργήσουν ταυτόχρονα macroticks, συντονίζοντας έτσι και τα δεδομένα τους. Η ακριβής διάρκεια της μονάδας καθορίζεται από τον σχεδιαστή και συνήθως είναι περίπου 1μs. Ως μικρότερη μονάδα σε κάθε κόμβο, ορίζεται το microtick, το οποίο υπολογίζεται βάσει του τοπικού ρολογιού. Είναι διαφορετικό σε κάθε cluster και αποτελεί τοπική μονάδα χρόνου.

3.4.2 Στάδια Κύκλου

Μια επικοινωνία απαρτίζεται από έναν αριθμό κύκλων επικοινωνίας, οι οποίοι αριθμούνται από 0 έως gCycleCountMax. Κάθε κύκλος αποτελείται από το στατικό τμήμα, το δυναμικό τμήμα, το παράθυρο συμβόλων και το χρόνο αδράνειας (Εικόνα 17).



Εικόνα 17 Στάδια κύκλου επικοινωνίας FlexRay [10]

Το πρώτο και το τελευταίο είναι υποχρεωτικά σε κάθε κύκλου, ενώ τα δύο ενδιάμεσα μπορεί να παραλείπονται. Ένας κύκλος χαρακτηρίζεται από σταθερό χρόνο διάρκειας τον οποίο προκαθορίζει ο σχεδιαστής του δικτύου και συνήθως είναι μεταξύ 1-5 ms. Επίσης προκαθορισμένες και σταθερές είναι και οι διάρκειες του στατικού και δυναμικού τμήματος. Το στατικό τμήμα αποτελείται από χρονοθυρίδες σταθερού και προκαθορισμένου πλήθους ίσης και επίσης σταθερής και προκαθορισμένης διάρκειας. Κάθε χρονοθυρίδα καθορίζεται από τον αριθμό χρονοθυρίδας (Slot Identifier, Slot ID). Το δυναμικό τμήμα έπεται του στατικού και διακρίνεται σε mini-slots. Η μετάδοση εδώ δεν βιάζεται, αλλά πραγματοποιείται μόνο όταν το απαιτεί κάποιο γεγονός (event-triggered). Οι μεταδόσεις ακολουθούν συγκεκριμένο σχήμα προτεραιοτήτων βάσει του αναγνωριστικού του πλαισίου. Αμέσως μετά ακολουθεί το παράθυρο συμβόλων, δηλαδή ένα διάστημα που χρησιμοποιείται για να επιβεβαιώσει τη λειτουργία των τοπικών bus guardians. Ο κύκλος ολοκληρώνεται με τον διάστημα αδράνειας του δικτύου, που είναι υπολειπόμενος χρόνος για να ολοκληρωθεί ο κύκλος. Σ' αυτόν δεν γίνεται κάτι πάνω στο κανάλι, δίνοντας την δυνατότητα για συγχρονισμό των τοπικών ρολογιών των κόμβων. Στο τέλος του

υπολογίζεται κάθε φορά ένα «offset», η λειτουργικότητα του οποίου αναλύεται στην επόμενη ενότητα του συγχρονισμού.

3.4.3. Συγχρονισμός

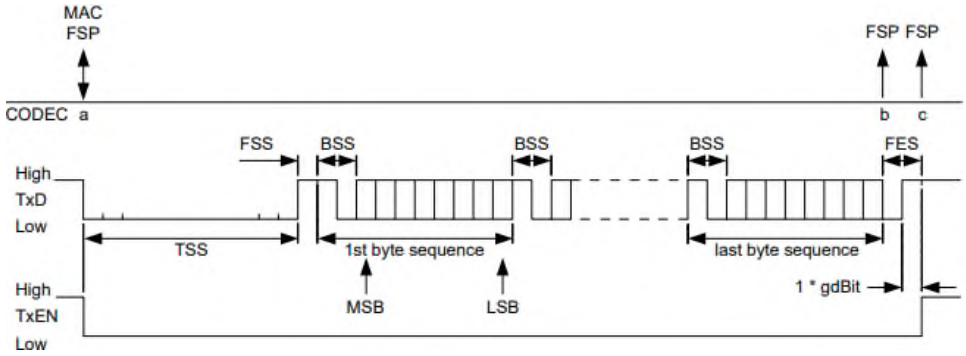
Στο FlexRay ο συγχρονισμός επιτυγχάνεται με startup και synch πλαίσια και όχι με εξωτερικά σήματα ρολογιών. Ένας coldstart κόμβος εκκινεί την μετάδοση βασισμένος στο τοπικό του ρολόι και σε κατάσταση listen ελέγχει το κανάλι για κίνηση πλαισίων. Επίσης μεταδίδει ένα σήμα αποφυγής συγκρούσεων (Collision Avoidance Symbol, CAS), ενημερώνοντας του υπόλοιπους πως είναι ο κυρίαρχος coldstart κόμβος. Ως κυρίαρχος, μεταδίδει πλαίσια εκκίνησης της επικοινωνίας σ' όλους τους άλλους κόμβους για τουλάχιστον 4 κύκλους επικοινωνίας και στα δύο κανάλια. Οι υπόλοιποι κόμβοι μεταδίδουν κατόπιν πλαίσια συγχρονισμού ώστε να επιτευχθεί ο συγχρονισμός. Κάθε πλαίσιο εκκίνησης είναι και πλαίσιο συγχρονισμού ώστε οι κόμβοι να υπολογίζουν την διαφορά μεταξύ των sync πλαισίων και να επαληθεύουν τα πλαίσια προς μετάδοση. Όπως προαναφέρθηκε στο τέλος του διαστήματος αδράνειας υπολογίζεται ένα «offset correction». Σκοπός του είναι να συγχρονίσει τον χρόνο εκκίνησης του κύκλου επικοινωνίας. Παρότι υπολογίζεται σε κάθε κύκλο, λαμβάνεται υπόψιν μόνο στους περιττούς κύκλους. Ο συγχρονισμός είναι αποτέλεσμα πρόσθεσης ή αφαίρεσης microticks από το «offset correction portion».

3.5 Μηχανισμοί Επικοινωνίας

Στο φυσικό επίπεδο του δικτύου κάθε τμήμα του κύκλου έχει συγκεκριμένους μηχανισμούς κωδικοποίησης και αποκωδικοποίησης μηνυμάτων και συμβόλων. Στην υποενότητα αυτή, παρουσιάζονται περιληπτικά οι μηχανισμού του στατικού τμήματος για την μετάδοση και την λήψη. Μικρές διαφορές παρατηρούνται στην περίπτωση του δυναμικού.

3.5.1 Κωδικοποίηση Πλαισίου

Ένα πλαίσιο δεν μεταδίδεται ως έχειν αλλά εμφωλεύεται σε ένα πακέτο, που δεν είναι τίποτα άλλο από μερικά bits πριν και μετά απ' αυτό (**Εικόνα 18**).



Εικόνα 18 Κωδικοποίηση πλαισίου FlexRay [2]

Πριν από το πλαίσιο μετάδοσης προστίθενται 5-15 bits πληροφορίας αρνητικού παλμού, που αποτελούν την ακολουθία εκκίνησης μετάδοσης (Transmit Start Sequence, TSS) και αμέσως μετά ένα ψηφίο θετικού παλμού που σηματοδοτεί την έναρξη του πλαισίου (Frame Start Sequence, FSS). Ο ρόλος της ακολουθίας έναρξης πλαισίου είναι να αντισταθμίσει κάποιο πιθανό σφάλμα κβαντισμού στην αρχή της ακολουθίας εκκίνησης. Αμέσως μετά ακολουθεί το πλαίσιο, το οποίο όμως χωρίζεται σε ομάδες από Bytes. Κάθε ομάδα περιβάλλεται από την ακολουθία έναρξης Bytes (Byte Start Sequence, BSS) που χρησιμοποιείται για την παροχή πληροφοριών χρονισμού ροής ψηφίων στις συσκευές λήψης του μηνύματος. Και οι δύο ακολουθίες έναρξης Byte αποτελούνται από ένα θετικό και ένα αρνητικό παλμό και βρίσκονται στην αρχή και στο τέλος κάθε ομάδα Bytes. Το τέλος του πλαισίου έπονται μερικά ψηφία αρνητικού και θετικού παλμού, λειτουργώντας ως ακολουθία τερματισμού (Frame End Sequence, FES).

3.5.2 Διαδικασία Μετάδοσης

Με την εκκίνηση του στατικού τμήματος ο κόμβος ενημερώνεται για το μετρητή χρονοθυρίδας (vSlotCounter) και καθορίζει το σημείο δράσης (action point) και τα όρια της θυρίδας (slot boundaries). Ο vSlotCounter αρχικοποιείται στην τιμή 1 και αυξάνεται κατά μια μονάδα στα όρια του κάθε θυρίδας. Η μέγιστη τιμή του είναι gNumberOfStatiSlots, η οποία είναι γνωστή σ' όλους τους κόμβους ενός cluster. Στην περίπτωση που θέλει να μεταδώσει πληροφορία, συναρμολογεί το πλαίσιο και αναμένει το σημείο δράσης. Αν δεν επιθυμεί μετάδοση καταφεύγει απευθείας στην αναμονή του σημείου δράσης. Η τιμή του αναγνωριστικού πλαισίου καθορίζεται από την τιμή του μετρητή χρονοθυρίδας την στιγμή της μετάδοσης. Άρα όταν

δημιουργείται ένα πλαίσιο η τιμή του καθορίζεται λίγο πριν την στιγμή της μετάδοσης. Μόλις φτάσει το σημείο δράσης, αν έχει κάτι να μεταδώσει το μεταδίδει και εν συνεχεία αναμένει το όριο της χρονοθυρίδας, στο τέλος της οποίας πραγματοποιείται η ενημέρωση του μετρητή.

3.6 Διαχείριση Σφαλμάτων

Οι μηχανισμοί διαχείρισης σφαλμάτων του FlexRay χρησιμοποιούν τρείς καταστάσεις για την αποφυγή προβλημάτων και τον περιορισμών των συνεπειών, την κανονική ενεργή, την κανονική παθητική και αυτή της παύσης. Στην πρώτη ο κόμβος θεωρείται πως λειτουργεί σωστά χωρίς προβλήματα ή κινδύνους. Στην παθητική ο κόμβος τίθεται σε περιορισμό και δεν του επιτρέπεται η εκπομπή πληροφοριών, καθώς εγκυμονεί ο κίνδυνος συγκρούσεων και σφαλμάτων συγχρονισμού. Η τρίτη, η κατάσταση παύσης ενεργοποιείται όταν τα σφάλματα που ανιχνεύτηκαν θεωρήθηκαν ιδιαιτέρως σοβαρά και κρίσιμα για την εύρυθμη λειτουργία του πρωτοκόλλου. Η κατάσταση του κόμβου αυτού μπορεί να αποκατασταθεί μόνο με επανεκκίνηση του. Προκειμένου να επιβληθούν οι καταστάσεις αυτές θα πρέπει να υπάρχει ένας μηχανισμός διαχείρισης που θα λειτουργεί ως διαιτησία. Το FlexRay διαθέτει δύο από αυτούς. Ο πρώτος υιοθετεί ένα μοντέλο υποβάθμισης στηριζόμενο στην εναλλαγή μεταξύ των και τριών, προκειμένου να υπάρχει ομαλή και σταδιακή μετάβαση στην κατάσταση παύσης. Ο δεύτερος χρησιμοποιείται για σημαντικά σφάλματα και προκαλεί μεταβάσεις απευθείας σε καταστάσεις παύσης.

Κεφάλαιο 4 Διανύσματα Επίθεσης και Ανίχνευση

4.1 Τύποι Επιθέσεων

Ορισμένες από τις πιο διαδομένες επιθέσεις που βρίσκουν εφαρμογή στη κυβερνοασφάλεια των οχημάτων είναι οι εξής:

- ***Packet Sniffing/Eavesdropping***: χρησιμοποιείται για τη μη εξουσιοδοτημένη παρακολούθηση της κίνησης δεδομένων πάνω στο δίκτυο, προκειμένου να εξακριβωθεί ο τρόπος επικοινωνίας μεταξύ των ECU. Τα πακέτα που ανταλλάσσονται συλλέγονται χωρίς να αφαιρούνται από το δίκτυο και με κατάλληλα εργαλεία αναλύονται και προβάλλονται στον επιτιθέμενο. Έτσι μπορούν να συλλεχθούν ευαίσθητα δεδομένα ή να συγκεντρωθούν πληροφορίες για την αρχιτεκτονική και τις παραμέτρους του δικτύου και των συμμετεχόντων σε αυτό κόμβων.
- ***Packet Fuzzing*** περιλαμβάνει την μετάδοση τυχαίων, λανθασμένων ή απρόσμενων μηνυμάτων στο δίκτυο προκειμένου να προκαλέσει κάποια απρόσμενη συμπεριφορά, απώλεια πόρων ή εκδήλωση σφαλμάτων, αποκαλύπτοντας έτσι ευπάθειες ασφαλείας στο σύστημα.
- ***ECU Flashing*** είναι μια τεχνική που περιλαμβάνει λογισμικό για reverse engineering προκειμένου προστεθεί επιπλέον λειτουργικότητα στην ECU πέραν της υπάρχουσας. Το πηγαίο λειτουργικό λογισμικό της μονάδας εξάγεται, αναλύεται με τα κατάλληλα εργαλεία, τροποποιείται από τον μηχανικό, μεταγλωττίζεται και φορτώνεται και πάλι πίσω στην μονάδα.
- ***Message Injection***: αφορά στην εισαγωγή στο δίαυλο του δικτύου ψευδών μηνυμάτων. Συνήθως στοχεύει στην διαρροή πληροφοριών, στη εκτέλεση ή μη εξουσιοδοτημένων ενεργειών ή στον αποπροσανατολισμό του στόχου λόγω ενημέρωσης με λανθασμένα δεδομένα.
- ***Message Modification***: Όμοιο με την έγχυση μηνύματος, μόνο που σε αυτήν την περίπτωση το μήνυμα δεν δημιουργείται και εισάγεται στο δίκτυο, αλλά τροποποιείται. Εφαρμόζεται σε μηνύματα που κυκλοφορούν στο δίαυλο. Αρχικά το μήνυμα συλλέγεται και εν συνεχεία τροποποιείται κατάλληλα ανάλογα των σκοπό που θέλει να εξυπηρετήσει.

- ***Message Replay***: ο επιτιθέμενος αφού συλλέξει μερικά από τα μηνύματα που κυκλοφορούν στο δίκτυο, επιλέγει ένα και το επαναπροωθεί συνεχώς προς τον προορισμό. Αποτέλεσμα ο στόχος να λαμβάνει τα ίδια ξανά και ξανά και έτσι να προκαλούνται διάφορες ακούσιες συνέπειες και κίνδυνοι στην ακεραιότητα του συστήματος.
- ***Physical Attack***: απαιτεί τη φυσική σύνδεση στο δίκτυο. Στοχεύει στην χειραγώγηση του υλικού του δικτύου όπως ο δίαυλος, οι bus guardians , οι ελεγκτές κτλ.
- ***Bus off Attack***: σκοπός της επίθεσης αυτής είναι ο κόμβος να βγει εκτός δικτύου μέσω σφαλμάτων. Τα σφάλματα που προκαλούνται θέτουν τον κόμβο σε κατάσταση που είναι ανίκανος να επικοινωνήσει είτε λόγο δυσλειτουργίας είτε λόγω απόρριψης από τους υπόλοιπους συμμετέχοντες στο δίκτυο κόμβους, ως μη ασφαλή
- ***Denial of Service (DoS)***: πολύ διαδεδομένη επίθεση στο δίκτυο που σταματά την σωστή λειτουργία του δικτύου μέσω καταιγισμού αιτήσεων. Αποτέλεσμα το δίκτυο ή οι κόμβοι οι οποίοι δέχονται τις αιτήσεις να μπλοκάρουν καθώς αδυνατούν να τις εξυπηρετήσουν. Συνήθως προκαλείται από συσσώρευση αιτήσεων γνωστό ως flooding είτε από εξάντληση του διαθέσιμου εύρους το δικτύου (bandwidth exhaustion).
- **Spoofing/Impersonation/Masquerading:** αφορά στην χειραγώγηση μιας αυθεντικής πηγής ή την δημιουργία μιας που αλληλεπιδρά ως αυθεντική ώστε να στείλει στοχευμένα κακόβουλα μηνύματα.
- ***Man-in-the-Middle Attack (MitM)***: ο όρος αναφέρεται σε τεχνικές επιθέσεων που εφαρμόζονται από έναν κόμβο που βρίσκεται εκτός δικτύου και παρεμβάλλεται μεταξύ της επικοινωνίας των αυθεντικών κόμβων. Σκοπός της επίθεσης είναι η διακοπή της επικοινωνίας ή παρακολούθηση της ή ακόμη και η παρεμβολή σε αυτήν. Ο κόμβος που δέχεται την επίθεση χαρακτηρίζεται ως Node under Attack (NUA).

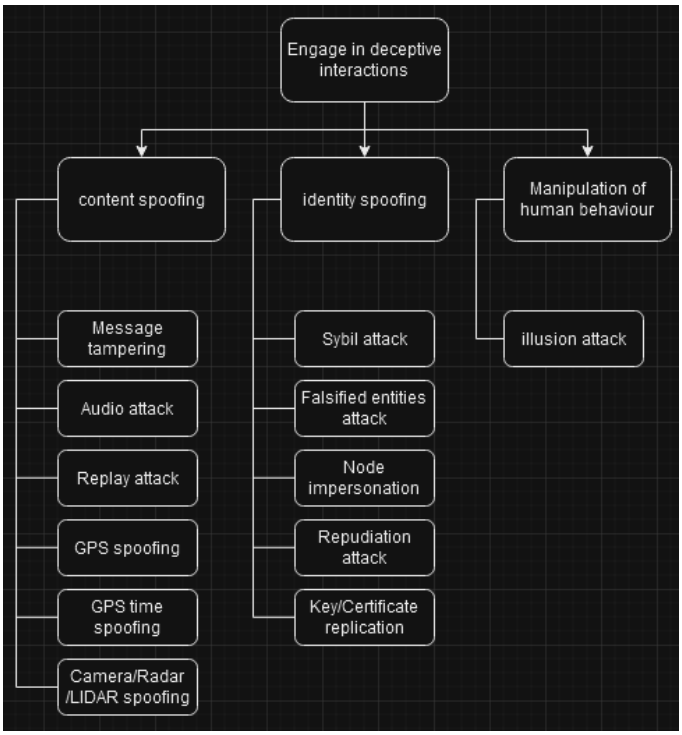
4.2 Διανύσματα Επίθεσης σε FlexRay

Ο ακριβής μηχανισμός της επίθεσης είναι άμεση εξάρτηση του σκοπού της. Στις ακόλουθες υπό-ενότητες αναλύονται τα διανύσματα επίθεσης, όπως αυτά

ταξινομούνται στο άρθρο "*A taxonomy of attack mechanisms in the automotive domain*" [3].

4.2.1 Engage in Deceptive Interaction

Προκειμένου να πείσει την άλλη μεριά πως επικοινωνεί με αυθεντική πηγή. Αυτό επιτυγχάνεται είτε με πλαστογράφηση περιεχομένου (content spoofing) είτε με πλαστογράφηση της ταυτότητας (identity spoofing) είτε με χειραγώγηση της ανθρώπινης συμπεριφοράς (manipulation of human behavior). Οι διαθέσιμες επιλογές σε κάθε σενάριο συνοψίζονται στη παρακάτω εικόνα (**Εικόνα 19**).



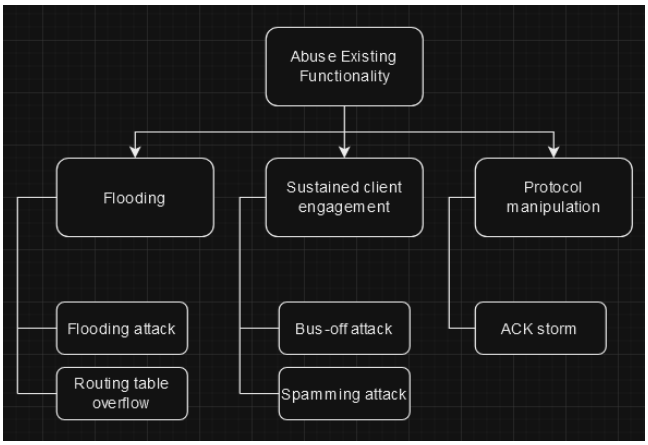
Εικόνα 19 Συμμετοχή σε παραπλανητικές αλληλεπιδράσεις

Στην περίπτωση πλαστογράφησης περιεχομένου ο επιτιθέμενος φέρνει σε επαφή το θύμα με ένα φαινομενικά αυθεντικό περιεχόμενο. Αυτό μπορεί να επιτευχθεί με πλαστά μηνύματα ειδοποιήσεων (Message tampering), ήχου (Audio attack), σήματος GPS (GPS spoofing), δεδομένων από αισθητήρες (Camera/Radar/LIDAR spoofing) ή με επανάληψη μηνύματος (replay attack) και χρονικής τροποποίησης των σημάτων του γεωεντοπισμού (GPS time spoofing). Για την παραβίαση της ταυτότητας ο επιτιθέμενος μπορεί να δημιουργήσει πολλαπλούς κόμβους ώστε να παραπλανήσει τους κόμβους του δικτύου (Falsified Entities attack) ή για να επηρεάσει την αξιοπιστία του δικτύου και να αποκτήσει δυσανάλογη επιρροή (Sybil attack). Επίσης δύναται να

προσποιηθεί τη συμπεριφορά ενός αυθεντικού κόμβου προκειμένου να γίνει αποδεχτός ως μέρος του δικτύου (Node impersonation), να αρνηθεί συστηματικά ενέργειες που ο ίδιος εκτελεί (Repudiation attack) ή να αντιγράψει κλειδιά και πειστήριά κρυπτογράφησης (Key/Certification Replication).

4.2.2 Abuse Existing Functionality

Από τους πιο διαδεδομένους τρόπους παρενόχλησης της λειτουργικότητας είναι η υπερφόρτωση του δικτύου (Flooding), η διαρκής δέσμευση των αυθεντικών κόμβων (Sustained client engagement) και η χειραγώγηση του πρωτοκόλλου (Protocol manipulation) μέσω της συστηματικής αποστολής μηνυμάτων επιβεβαίωσης (ACK storm). Στην πρώτη μέθοδο οι επιλογές είναι είτε ο κατακλυσμός του δικτύου με μηνύματα και αιτήματα (Flooding attack) είτε η υπερχείλιση του πίνακα δρομολόγησης (Routing table overflow) και στοχεύει στο να καταστήσει το κόμβο μη λειτουργικό. Στη διακοπή ή στη καταπόνηση της επικοινωνίας, στοχεύουν οι επιθέσεις της δέσμευσης των κόμβων, η οποία είναι δυνατή είτε μέσω του συνεχούς βομβαρδισμού του με μηνύματα (Spamming attack) είτε με την πρόκληση σφαλμάτων που θα τον εξαιρέσουν από το δίκτυο (Bus-off attack). Οι επιλογές παρουσιάζονται στην ακόλουθη εικόνα (**Εικόνα 20**).

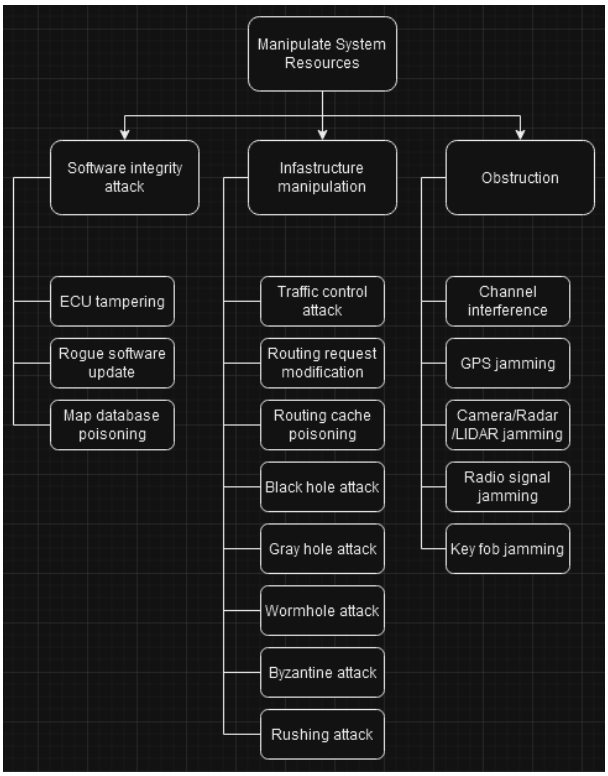


Εικόνα 20 Παρενόχληση υπάρχουσας λειτουργικότητας

4.2.3 Manipulate System Resources

Αφορά στη χειραγώγηση των πόρων του δικτύου (**Εικόνα 21**) προκειμένου να εξυπηρετηθούν συγκεκριμένοι σκοποί και περιλαμβάνει επιθέσεις ακεραιότητας λογισμικού (Software integrity), χειραγώγησης υποδομών (Infrastructure manipulation) ή παρεμπόδιση (Obstruction). Η τελευταία περίπτωση επιτυγχάνεται

μέσω της εφαρμογής στο κανάλι θορύβου ή παρεμβολών (Channel interference), την μετάδοση σημάτων απόκρυψης (jamming attacks) των σημάτων GPS, των αισθητήρων, του ραδιοφώνου ή των ασύρματων κλειδιών.

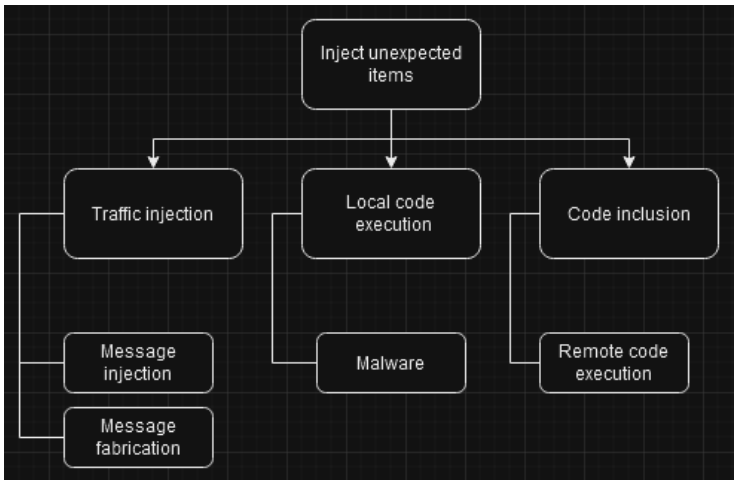


Εικόνα 21 Χειραγώγηση πόρων συστήματος

Ο μη εξουσιοδοτημένος χειρισμός και έλεγχος μιας HME (ECU tampering), η κακόβουλη ενημέρωση λογισμικού (Rogue software update) και η μόλυνση των βάσεων δεδομένων που περιέχουν πληροφορίες των χαρτών (Map database poisoning) έχουν ως στόχο την παράκαμψη μέτρων ασφαλείας και την εξάντληση των πόρων του οχήματος. Επιθέσεις σε υποδομές αφορούν τον έλεγχο της κυκλοφορίας του δικτύου (Traffic control), την αναδιανομή των πακέτων αιτήσεων δρομολόγησης χωρίς επεξεργασία (Rushing attack), την τροποποίηση των αιτημάτων δρομολόγησης (Routing request modification) ή την μόλυνση των προσωρινών μνημών αυτών (Routing cache poisoning). Επιπρόσθετα στην κατηγορία αυτή υπόκεινται η δημιουργία κενών στην επικοινωνία (Black hole), η επανάληψη μηνυμάτων από ένα σημείο του δικτύου σε άλλο παραβιάζοντας χωρικές και χρονικές ακεραιότητες (Wormhole) καθώς και η τροποποίηση επιλεκτικών δεδομένων πάνω στο δίκτυο (Gray hole). Τέλος η συνεργασία κόμβων στο δίκτυο για την εξάντληση των πόρων (Byzantine attack) ανήκει και αυτή στη περίπτωση τα χειραγώγησης των υποδομών.

4.2.4 Inject Unexpected Items

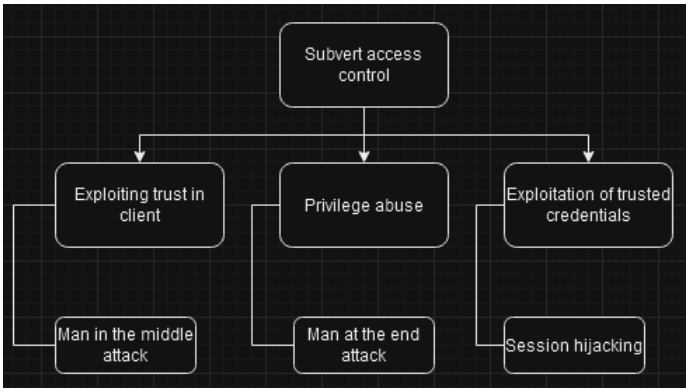
Οι εισαγωγή απρόσμενου περιεχομένου σε ένα δίκτυο ενός ευφυούς και συνδεδεμένου οχήματος επιτυγχάνεται, με τα διανύσματα της **Εικόνα 22**, δηλαδή με την έγχυση στη κυκλοφορία του δικτύου, την εκτέλεση τοπικού κώδικα ή την συμπερίληψη κώδικα μέσω απομακρυσμένης εκτέλεσης (Remote code execution). Η έγχυση περιλαμβάνει εισαγωγή έτοιμου μηνύματος απευθείας στο κανάλι (message injection) ή στην κατασκευή ενός που μοιάζει αυθεντικό (message fabrication). Η εκτέλεση κώδικα τοπικά, απαιτεί μόλυνση της μονάδας με κακόβουλο λογισμικό (malware).



Εικόνα 22 Εισαγωγή απρόσμενων αντικειμένων

4.2.5 Subvert Access Control

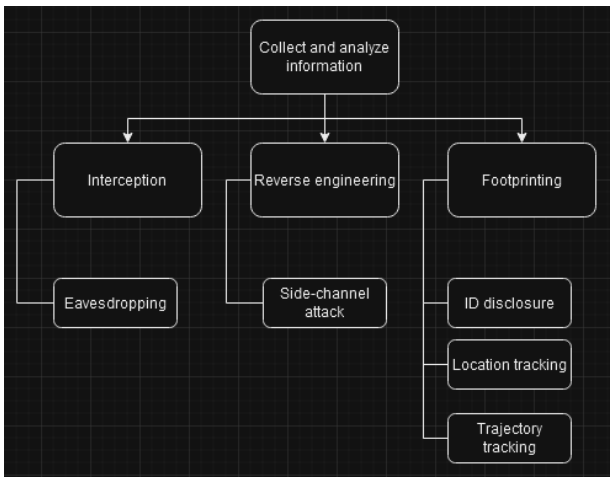
Η υπονόμευση του ελέγχου πρόσβασης (**Εικόνα 23**) μέσω της εκμετάλλευσης της εμπιστοσύνης στον πελάτη (Exploiting trust in client) ή της κατάχρησης προνομιούχων δικαιωμάτων (Privilege access) μπορεί να επιτευχθεί με την παρεμβολή ενός κόμβου ανάμεσα σε δύο αυθεντικούς (Man-in-the-middle attack) ή μέσω της χρήσης της αδειοδοτημένης πρόσβασης της μιας πλευράς (Man-in-the-end attack) αντίστοιχα. Η πρώτη αποσκοπεί στην αλλοίωση της επικοινωνίας ή την υπόκλεψη δεδομένων και στοιχείων των συμμετεχόντων στην επικοινωνία και η δεύτερη στην απόκτηση πρόσβασης σε ευαίσθητες πηγές και την διάπραξη ενεργειών χωρίς συναίνεση. Τέλος η εκμετάλλευση αξιόπιστων διαπιστευτηρίων (Exploitation of trusted credentials) απαιτεί την πειρατεία της συνεδρίας (Session hijacking), δηλαδή του πλήρη ελέγχου μιας ενεργής συνεδρίας.



Εικόνα 23 Υπονόμευση ελέγχου πρόσβασης

4.2.6 Collect and Analyze Information

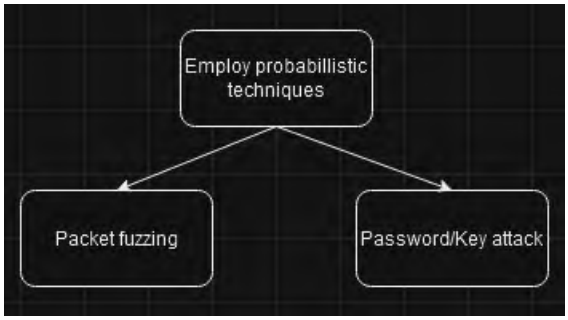
Ένας από τα πρώτα βήματα ενός επιτιθέμενου είναι η συλλογή και ανάλυση δεδομένων. Όπως φαίνεται από την **Εικόνα 24**, αυτή είναι δυνατή μέσω της παρακολούθησης του δίαυλου επικοινωνίας (Eavesdropping) που επιτρέπει τη συλλογή, την ανάλυση ή την ανακοπή μηνυμάτων. Επίσης είναι δυνατή μέσω της αντιστροφής μηχανικής (Reverse engineering), μιας διαδικασίας που αφορά στη ανάκτηση του πηγαίου κώδικα και των εσωτερικών δομών ενός συστήματος. Επιτυγχάνεται με φυσική σύνδεση στο μέσο και διαρροή πληροφοριών με επιθέσεις πλευρικού καναλιού (Side-channel attack) που περιλαμβάνουν χρονισμό, κατανάλωση ισχύος ή εκπομπή ηλεκτρομαγνητικών σημάτων. Τέλος η συλλογή και ανάλυση είναι δυνατή μέσω της καταγραφής των αποτυπωμάτων της δραστηριότητας (Foot printing) ενός μέσου που επιτυγχάνεται μέσω της αποκάλυψης των αναγνωριστικών (ID disclosure), του εντοπισμού την τοποθεσίας (Location tracking) ή την καταγραφή της τροχιάς του οχήματος (Trajectory tracking).



Εικόνα 24 Συλλογή και ανάλυση πληροφορίας

4.2.7 Employ Probabilistic Techniques

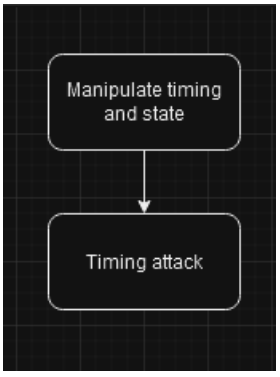
Το διάνυσμα αυτό αφορά στην εφαρμογή τεχνικών πιθανότητας (**Εικόνα 25**) προκειμένου να καμφθούν μέτρα ασφαλείας. Εφαρμόζεται με δύο τρόπους, μέσω της μετάδοσης τυχαίων, εσφαλμένων ή απρόσμενων μηνυμάτων σε ένα σύστημα με απώτερο σκοπό της εμφάνιση ευπαθειών (packet fuzzing) ή μέσω της προσπάθειας εκτίμησης και εξαγωγής των σωστών διαπιστηρίων και κλειδιών (Password/key attack). Και οι δύο στηρίζονται σε στατικούς αλγορίθμους και μαθηματικά μοντέλα πιθανοτήτων.



Εικόνα 25 Εκμετάλλευση τεχνικών πιθανότητας

4.2.8 Manipulate Timing and State

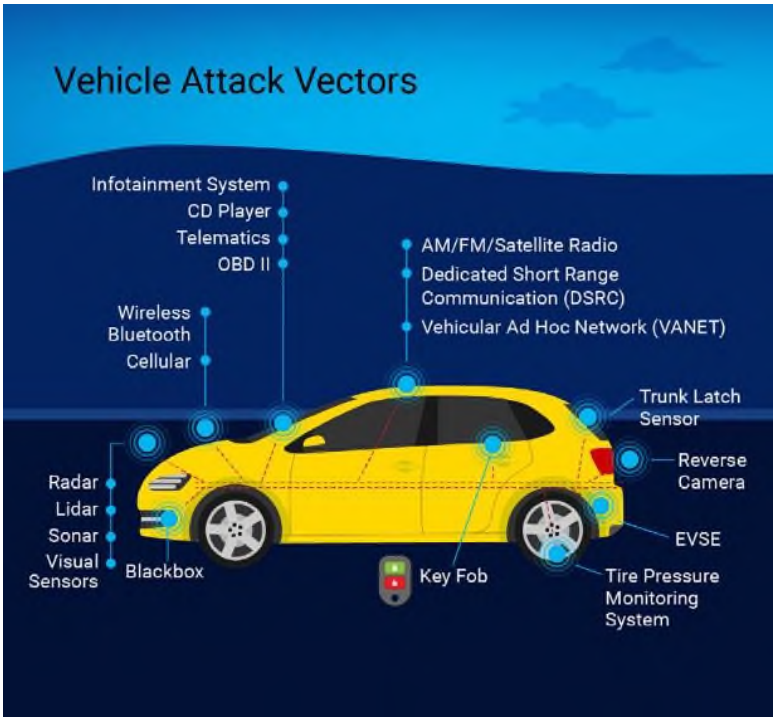
Η επίθεση στο όχημα, μέσω αυτού του διανύσματος (**Εικόνα 26**) αποσκοπεί στον έλεγχο του χρονισμού των ενεργειών και των καταστάσεων του συστήματος. Εφαρμόζεται μόνο με επίθεση βασισμένη στο χρόνο (Timming attack), η οποία εκμεταλλεύεται την απόκριση ή την καθυστέρηση κατά την εκτέλεση μιας λειτουργίας ή υπηρεσίας.



Εικόνα 26 Χειραγώγηση χρόνου και καταστάσεων

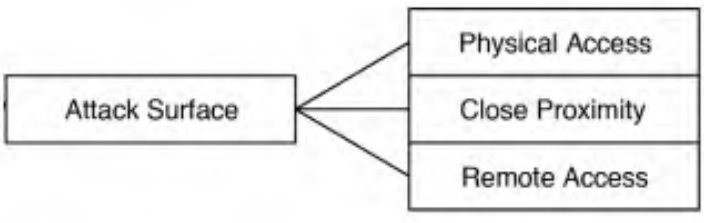
4.3 Entry Points

Δεδομένων των κύριων αρχιτεκτονικών και των διανυσμάτων επίθεσης της προηγούμενης ενότητας (**4.2 Διανύσματα Επίθεσης σε FlexRay**) ένας εισβολέας μπορεί να αξιοποιήσει πολλαπλά σημεία εισόδου στο όχημα (**Εικόνα 27**) για να πετύχει τον στόχο του.



Εικόνα 27 Ταξινόμηση των entry points [27]

Τα σημεία αυτά μπορούν να κατηγοριοποιηθούν σε τρείς τύπους (**Εικόνα 28**) βάση της εγγύτητας, δηλαδή σε άμεση φυσική πρόσβαση, σε άμεση φυσική πρόσβαση και σε απομακρυσμένη.



Εικόνα 28 Επιφάνειες επιθέσεων [3]

4.3.1 Direct Physical Access

Ο πρώτος τρόπος πρόσβασης αναφέρεται στα τρωτά σημεία και τους κινδύνους που σχετίζονται με την απευθείας φυσική πρόσβαση στα αρχιτεκτονικά στοιχεία του οχήματος. Αυτός περιλαμβάνει την σύνδεση στα δίκτυα επικοινωνίας και στις ηλεκτρονικές μονάδες ελέγχου με σκοπό να αποκαλύψει πολλές πληροφορίες και να επιτρέψει στον επιτιθέμενο να χειρίζεται πολλαπλές λειτουργίες του οχήματος. Παραδείγματα περιλαμβάνουν επιθέσεις ανάγνωσης μνήμης που επιτρέπουν την ανάκτηση λογισμικού για reverse engineering και παραμέτρων διαμόρφωσης, οι οποίες αποτελούν παραβίαση της ιδιωτικότητας των επιλογών του κατασκευαστή. Η πρόσβαση σε εξωτερικά στοιχεία μνήμης των ECU μπορεί επίσης να παραχωρήσει στον επιτιθέμενο δικαίωμα εγγραφής, το οποίο μπορεί να εκμεταλλευτεί για να τροποποιήσει το λογισμικό του ECU. Η πρόσβαση αυτή είναι δυνατή είτε μέσω υλικού που θα συνδεθεί στους διαύλους του δικτύου είτε μέσω υλικού που θα συνδεθεί στα πινάκια των ελεγκτών.

4.3.2 Indirect Physical Access

Ένας επιτιθέμενος μπορεί να έχει πρόσβαση στο όχημα μέσω συσκευών που αποτελούν μέρος του εξοπλισμού του. Σε αυτές περιλαμβάνονται τα πολυμέσα , το σύστημα infotainment και η θύρα OBD-II. Τα ευφυή οχήματα διαθέτουν θύρες USB εξυπηρετούν διάφορες λειτουργίες όπως την αναπαραγωγή ήχου και βίντεο, την ενημέρωση του λογισμικού ή του υλικολογισμικού του υπολογιστή της οθόνης διεπαφής. Παρότι εξυπηρετούν σε μεγάλο βαθμό τους χρήστες αποτελούν πολύ εύκολο σημείο εισαγωγής κακόβολων λογισμικών. Η φόρτωση μολυσμένων αρχείων, μη εξουσιοδοτημένων λογισμικών ή κακόβουλων ενημερώσεων λογισμικού μπορούν να εκμεταλλευθούν ευπάθειες στο σύστημα ψυχαγωγίας και να θέσουν σε κίνδυνο είτε την ακεραιότητα των επιβατών ή την ιδιωτικότητα των δεδομένων τους. Αντίστοιχες δράσεις μπορούν να εξυπηρετηθούν και μέσω της αναπαραγωγής CD-ROM, DVD-ROM κτλ. Πολλές ευπάθειες και περιπτώσεις επιτυχημένων επιθέσεων έχουν αναφερθεί κυρίως από την χρήση των κινητών συσκευών. Οι κινητές συσκευές συνδέονται στα ευφυή οχήματα, μέσω λογισμικών που εκτελούνται και στις δύο πλευρές. Το γεγονός της σύνδεσης αυτής δίνει πληθώρα επιλογών στον επιτιθέμενο, αφού η εξυπηρέτηση των σκοπών του μπορεί να πραγματοποιηθεί με αποστολή

μηνυμάτων, με κακόβουλες εφαρμογές, μέσω επιθέσεων στις εφαρμογές των μέσων κοινωνικής δικτύωσης κ.ά. Τέλος η σύνδεση στην OBD-II θύρα (**Εικόνα 29**) απαιτεί μια πιο άμεση πρόσβαση από τις υπόλοιπες, στην οποία μάλιστα υπάρχει μεγάλη τεχνογνωσία και αρκετές διαθέσιμες πρακτικές και εργαλεία αφού αποτελεί μέσω για την αναβάθμιση και την τροποποίηση των λειτουργιών του οχήματος με απώτερο σκοπό την βελτίωση και προσαρμογή των επιδόσεων του.

Εικόνα 29 Φωτογραφίας μια θύρας OBD-II [21]

4.3.3 Remote Access

Η απομακρυσμένη ασύρματη πρόσβαση μπορεί να ταξινομηθεί σε δύο κατηγορίες, αυτές της μικρής και της μεγάλης εμβέλειας. Στην πρώτη υπόκεινται επιθέσεις που χρησιμοποιούν το Wi-Fi του οχήματος, το Bluetooth, τις ραδιοσυχνότητες (RF/RFID), την τεχνολογία επικοινωνίας μεταξύ οχημάτων Vehicle-to-Vehicle (V2V) ή την τεχνολογία Over-the-Air (OTA) ενημέρωσης κτλ. Για παράδειγμα οι πομποί για την ρύθμιση της πίεσης των ελαστικών TPMS ή τα παθητικά συστήματα πρόσβασης χωρίς κλειδί PKES, λειτουργούν σε ραδιοφωνικές συχνότητες μεταδίδοντας μηνύματα μικρής εμβέλειας που περιέχουν πληροφορία αυθεντικοποίησης και ταυτοποίησης. Στην δεύτερη κατηγορία συγκαταλέγονται το GPS και τα δίκτυα επικοινωνίας Vehicle-to-Infrastructure (V2I) και Vehicle-to-Everything (V2X). Η κατηγορία αυτή στηρίζεται στην εκμετάλλευση τρωτών σημείων στις δυνατότητες απομακρυσμένης συνδεσιμότητας του οχήματος και οι επιτιθέμενοι μπορούν να στοχεύσουν αδύναμους μηχανισμούς ελέγχου ταυτότητας και ανεπαρκώς ασφαλή συστήματα υποστήριξης για να αποκτήσουν μη εξουσιοδοτημένη απομακρυσμένη πρόσβαση

στα συστήματα του οχήματος, επιτρέποντας ενδεχομένως τον τηλεχειρισμό ή την κλοπή δεδομένων.

4.4 Επίθεση σε FlexRay

Λόγω της ντετερμινιστικότητας του πρωτοκόλλου, ο σχεδιασμός επίθεσης απαιτεί καλή γνώση του δικτύου, καθώς μια απλή απευθείας σύνδεση με τους διαύλους θα δώσει πρόσβαση μόνο στη τρέχουσα επικοινωνία. Ένα πλαίσιο που δεν έχει παραχθεί και μεταδοθεί από κόμβο FlexRay, προκειμένου να γίνει αποδεχτό από έναν άλλο κόμβο, δηλαδή τον Ελεγκτή Επικοινωνίας αυτού, θα πρέπει να περάσει τους ελέγχους για τις τιμές των κυκλικών ελέγχων πλεονασμού τόσο στην κεφαλή όσο και στην ουρά του πλαισίου και να τηρεί το χρονικό περιορισμό του κύκλου επικοινωνίας και της χρονοθυρίδας.

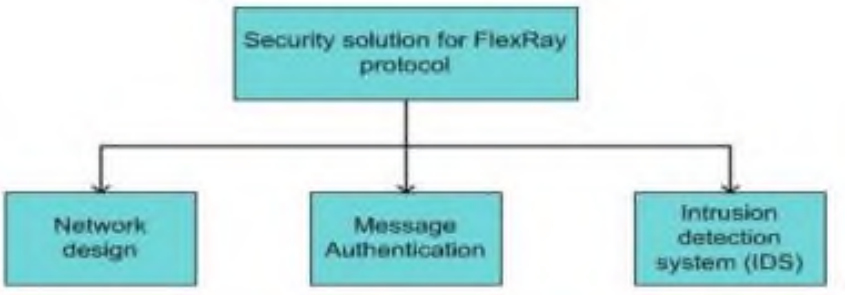
Η λειτουργικότητα του FlexRay στηρίζεται στην παραγωγή, από τον transceiver, συγκεκριμένων φυσικών σημάτων στο δίαυλο επικοινωνίας που αντιστοιχούν σε λογικές καταστάσεις του καναλιού. Για την διάκριση αυτών έχει προκαθορισμένα συγκεκριμένα thresholds τάσης. Το πρωτόκολλο δεν διαθέτει ενσωματωμένο μηχανισμό διαχείρισης των συγκρούσεων των δεδομένων. Κάθε χρονική στιγμή, υπό κανονικές συνθήκες λειτουργίες μόνο ένα κυρίαρχο σήμα επιτρέπεται να παραχθεί και οι υπόλοιποι κόμβοι παραμένουν αδρανείς. Κατά συνέπεια οι συγκρούσεις μπορούν να οδηγήσουν σε απρόβλεπτα επίπεδα τάσης και την δημιουργία αναταραχών στην εύρυθμη λειτουργία του πρωτοκόλλου. Στο φυσικό επίπεδο υλοποιείται μέρος του πρωτοκόλλου, το υπόλοιπο πραγματοποιείται στο επίπεδο της διασύνδεσης των δεδομένων με την ρύθμιση των παραμέτρων του.

Μια απειλή στο δίκτυο FlexRay μπορεί να είναι μονόδρομη (monodirectional) ή αμφίδρομη (bidirectional). Στην πρώτη περίπτωση ο επιτιθέμενος τροποποιεί ή επαναμεταδίδει δεδομένα που εξάγονται από έναν κόμβο προς τους υπόλοιπους. Συνεπώς η μόνη γνώση που χρειάζεται να διαθέτει είναι ποια πλαίσια και ποιες χρονοθυρίδες ανήκουν στον υπό επίθεση κόμβο (NUA). Η περίπτωση της αμφίδρομης επίθεσης αποτελεί δύο μονόδρομες για την μετάδοση προς και από τον NUA. Η φυσική υλοποίηση τον μηχανισμών θα εισάγει αναπόφευκτα μια καθυστέρηση.

4.5 Μηχανισμοί Ανίχνευσης σε FlexRay

4.5.1 Εισαγωγή

Η ανίχνευση επιθέσεων στο πρωτόκολλο επικοινωνίας FlexRay περιλαμβάνει την ανάπτυξη συγκεκριμένων μηχανισμών [62], ορισμένοι από τους οποίους είναι οι ακόλουθοι (**Εικόνα 30**).

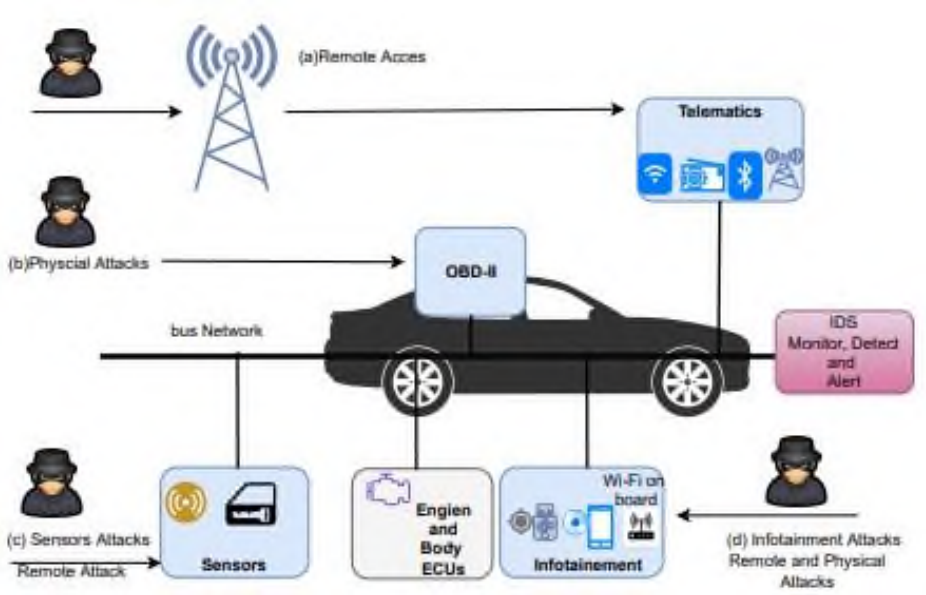


Εικόνα 30 Πιθανές λύσεις προστασίας του FlexRay [62]

Μελέτες έχουν δείξει πως η υιοθέτηση της σωστής τοπολογίας στο δίκτυο του FlexRay μπορεί να αποτρέψει από την εφαρμογή συγκεκριμένων επιθέσεων, όπως οι spoofed frame attacks ([62], [7]). Πολλοί όμως είναι και εκείνοι που υποστηρίζουν την ανάγκη για κρυπτογράφηση και κωδικοποίησης [55]. Μια λύση για αυθεντικοποίησης ενός μηνύματος είναι η εισαγωγή ενός κωδικού ταυτοποίησης στο τμήμα των δεδομένων [62]. Πολύ μεγαλύτερο ενδιαφέρον όμως φαίνεται να υπάρχει στα συστήματα ανίχνευσης εισβολέων IDS και μάλιστα με μηχανισμό βασισμένο στη αλγορίθμους μηχανικής μάθησης ([11], [15], [17], [18], [26], [66] κ.ά.).

4.5.2 Intrusion Detection Systems

Ένα σύστημα ανίχνευσης εισβολών παρακολουθεί τη κυκλοφορία των δεδομένων και τα εξετάζει σύμφωνα με πρότυπα και μοτίβα για ύποπτες συμπεριφορές. Σε περίπτωση εντοπισμού μιας κακόβουλης ενέργειας εκπέμπει ειδοποιήσεις για να ληφθούν μέτρα καταστολής (**Εικόνα 31**).



Εικόνα 31 Λειτουργία ενός IDS σε ένα ICV [24]

Τα συστήματα αυτά διακρίνονται βάσει της θέσης που τοποθετούνται σε Network IDS και Host IDS και βάσει του μηχανισμού ανίχνευσης σε Signature-based IDS και Anomaly-based IDS. Τα Network Intrusion Detection System (NIDS) τοποθετούνται σε στρατηγικά σημεία πάνω στο εσωτερικό δίκτυο επικοινωνίας του οχήματος και παρακολουθούν την κυκλοφορία των πακέτων σε αυτό. Αντιθέτως το Host Intrusion Detection System (HIDS) εκτελείται ανεξάρτητα σε έναν host ή σε μια συσκευή, παρακολουθώντας όλη τη πληροφορία που εξέρχεται και εισέρχεται από και σε αυτόν αντίστοιχα. Οι αλγόριθμοι ανίχνευσης ανωμαλιών εξετάζουν τα δεδομένα για πιθανές παρεκκλίσεις από την συνηθισμένη συμπεριφορά και είναι ικανές να εντοπίζουν νέες επιθέσεις, που δεν έχουν καταγραφεί προηγουμένως. Πρόκειται για λογισμικό που παρακολουθεί την κίνηση του δικτύου για ύποπτη ή κακόβουλη δράση. Συνήθως λειτουργούν μοντελοποιώντας την κανονική συμπεριφορά και εν συνεχεία συγκρίνοντας την με την τρέχουσα. Όταν η δεύτερη παρεκκλίνει τότε την εξετάζει ενδελεχώς και την ταξινομεί στις διάφορες κλάσεις ανωμαλίας. Στηρίζονται σε στατιστικές μεθόδους, αλγορίθμους μηχανικής μάθησης και σε μεθόδους βασισμένους σε κανόνες και φυσικά χαρακτηριστικά του πρωτοκόλλου. Η ανίχνευση βασισμένη σε υπογραφή στηρίζεται σε πρότυπες επιθέσεις με γνωστές υπογραφές και στοιχεία. Παρακολουθεί το δίκτυο με ανιχνευτές και σαρωτές. Τα στοιχεία αυτά έχουν ρυθμιστεί προηγουμένως με γνωστά μοτίβα και ακολουθίες επιθέσεων. Κάθε στιγμή συγκρίνει την εισερχόμενη πληροφορία με βάσεις δεδομένων γνωστών

επιθέσεων και αποφασίζει αν πρόκειται για κακόβουλη δράση. Έχει χαμηλό ποσοστό ψευδώς θετικών αξιολογήσεων, ωστόσο αποτυγχάνει να εντοπίσει νέες επιθέσεις και απαιτεί συνεχή ενημέρωση των βάσεων δεδομένων της.

Μια προσπάθεια ταξινόμησης των επιλογών κατά το σχεδιασμό ενός IDS εσωτερικής επικοινωνία στα ευφυή και συνδεδεμένα οχημάτα προσπάθησαν να κάνουν ο Georgios Karopoulos και συν. [49], βασισμένοι σε σχετικές εργασίες διαθέσιμες στη βιβλιογραφία όπως φαίνεται στην **Εικόνα 32**. Αυτές περιλαμβάνουν την ανίχνευση βάση υπογραφής και ανωμαλιών καθώς επίσης και με στατιστικά μοντέλα, αλγορίθμους μηχανικής μάθησης και τεχνικές βασισμένες στη θεωρία πληροφοριών. Λαμβάνουν υπόψιν τους την ανίχνευση βάση των κανόνων του πρωτοκόλλου όπως η συχνότητα, ο χρόνος και τα πεδία των πλαισίων και βάση των φυσικών χαρακτηριστικών των ECU όπως το clock offset, την διακύμανση της τάσης και τις ιδιαιτερότητες των σημάτων. Η ταξινόμηση περιέχει την διάκριση του συστήματος βάση του σημείου τοποθέτησης τους στο δίκτυο, όπως επίσης και του τύπου αντίδρασης και τρόπου επιβεβαίωσης που αυτό πρέπει αν έχει σε περιπτώσεις ανίχνευσης κακόβουλης ή ύποπτης δράσης.

Εικόνα 32 Ταξινόμηση μηχανισμών ενός IDS ενδοεπικοινωνίας

4.5.3 Machine Learning and IDS

Η μηχανική μάθηση σε ένα σύστημα ανίχνευσης εισβολέων μπορεί να προσφέρει πολλές επιλογές, από την εξαγωγή και εκμάθηση της κανονικής και ανώμαλης συμπεριφοράς μέχρι τον εντοπισμό και τη πρόβλεψη επιθέσεων. Για την εφαρμογή

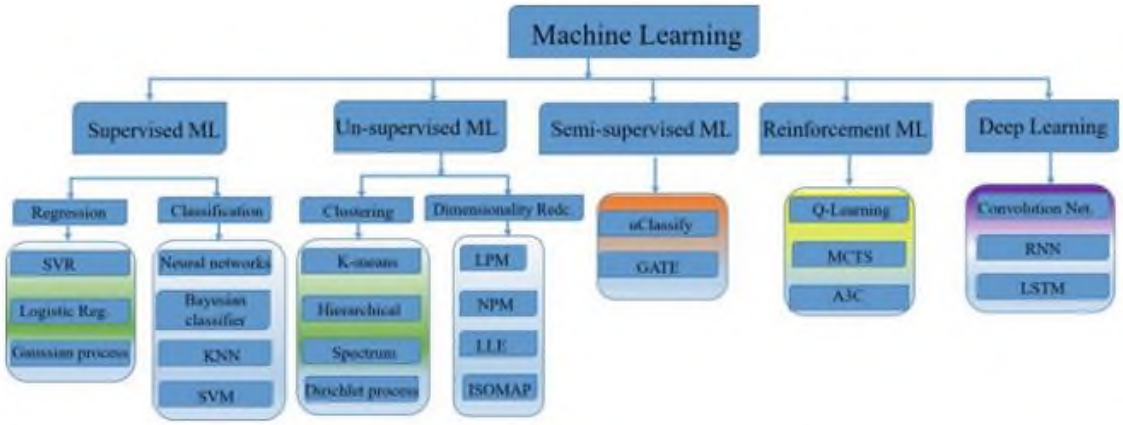
της όμως είναι απαραίτητος ο προσδιορισμός του μηχανισμού μάθησης που είναι κατάλληλος για την εφαρμογή (**Εικόνα 33**).

- Supervised Learning: βασίζεται στην άμεση εποπτεία της λειτουργίας και στόχος της είναι η μέτρηση του εύρους των δεδομένων και πρόβλεψης των άγνωστων, μη διαθέσιμων και μελλοντικών δεδομένων με βάση labeled δείγματα. Τα labels επιτρέπουν την εύρεση της ακριβούς σχέσης μεταξύ των σημείων. Σκοπός της μάθησης είναι η αντιστοίχιση του χώρου χαρακτηριστικών εισόδου στον χώρο των labels για την λήψη της επιθυμητής έξοδο. Όσο περισσότερα είναι τα δεδομένα εκπαίδευσης, τόσο μικρότερο είναι το ποσοστό σφάλματος. Λύνει δύο προβλήματα, αυτό της παλινδρόμησης (Regression) και αυτό της ταξινόμησης (Classification). Στο πρώτο προσδιορίζει τα μοτίβα και υπολογίζει τις προβλέψεις συνεχών αποτελεσμάτων ενώ στο δεύτερο τα δείγματα εισόδου γίνονται labeled με βάση προηγούμενα δείγματα και ο αλγόριθμος εκπαιδεύεται να αναγνωρίζει ορισμένους τύπους αντικειμένων και να τα ταξινομεί σε διακριτές εξόδους. Γνωστά μοντέλα για Regression είναι τα Support Vector Regression (SVR), Logistic Regression, Random Forecast, Gaussian Process κτλ. και για Classification τα Neural Networks, Bayesian Classifiers, k-Nearest Neighbors, Decision Trees, Support Vector Machines κτλ.
- Unsupervised Learning: λειτουργούν με unlabeled δεδομένα και άρα δεν απαιτούν ανθρώπινη εργασία για να γίνει το σύνολο δεδομένων αναγνώσιμο, επιτρέποντας έτσι την επεξεργασία πολύ μεγαλύτερων datasets. Οι σχέσεις μεταξύ των σημείων δεδομένων γίνονται αντιληπτές από τον αλγόριθμο με αφηρημένο τρόπο, χωρίς να απαιτείται κάποια είσοδος από τον άνθρωπο. Έτσι οι αλγόριθμοι αυτοί γίνονται πιο ευέλικτοι, δηλαδή δεν απαιτούν ακριβή δήλωση και να αποσαφήνιση του προβλήματος αλλά μπορούν να προσαρμόζονται στα δεδομένα δυναμικά αλλάζοντας τις κρυφές δομές. Χωρίζονται και πάλι σε δύο τύπους αυτούς που εκτελούν ομαδοποίηση (Clustering) και αυτούς που εκτελούν μείωση διαστάσεων (Dimensionality Reduction). Στη πρώτη περίπτωση τα unlabeled δείγματα ομαδοποιούνται σε διαφορετικές συστάδες ανάλογα με τις ομοιότητές τους ενώ στη δεύτερη ο

αλγόριθμος μειώνει την υψηλή διάσταση σε χαμηλή διάσταση αφαιρώντας τον ανεπιθύμητο θόρυβο από τα εισερχόμενα δεδομένα χωρίς όμως να οδηγηθεί σε απώλεια πληροφοριών. Παραδείγματα αλγορίθμων Clustering είναι ο K-means, Hierarchical clustering, Spectrum clustering κ.ά. και αλγορίθμων Dimensionality reduction οι Linear projection method (LPM), Nonlinear projection method (NPM), Local linear embedding (LLE) κτλ..

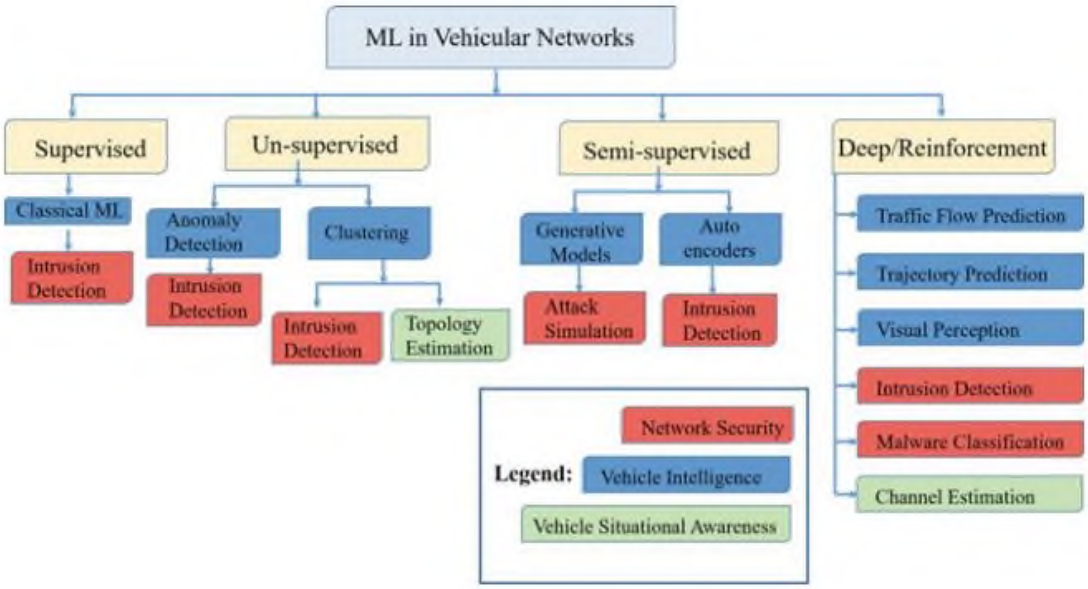
- Semi-supervised Learning: όπως υποδεικνύει και το όνομα πρόκειται για μια μέθοδο μηχανικής μάθησης που βρίσκεται μεταξύ της εποπτευόμενης και της μη εποπτευόμενης μηχανικής εκμάθησης. Η μάθηση αυτή αξιοποιεί το περιορισμένο διαθέσιμο αριθμό σε labeled δείγματα για να εκπαιδευτεί με μικρό πλήθος unlabeled δεδομένων, pseudo-labeled. Έπειτα συνδυάζει τα labeled και τα pseudo-labeled δείγματα για να σχεδιάσει έναν αλγόριθμο που αναπαριστά τα χαρακτηριστικά και των δύο προαναφερθέντων ειδών μάθησης. Βασίζεται σε μεθόδους Classification για να εντοπίσει τις ιδιότητες των δεδομένων και στην συνέχεια σε Clustering μεθόδους για να τα διακρίνει σε συγκεκριμένες ομάδες. Μερικά παραδείγματα αλγορίθμων είναι οι uClassify και ο General architecture for text engineering (GATE).
- Reinforcement Learning: αλγόριθμοι εμπνευσμένοι από τον μηχανισμό μάθησης του ανθρώπου, διαθέτουν έναν αλγόριθμο που βελτιώνεται μόνος του και μαθαίνει από νέες καταστάσεις χρησιμοποιώντας μια μέθοδο trial-and-error. Τα ευνοϊκά αποτελέσματα ενθαρρύνονται ή ενισχύονται και τα μη ευνοϊκά αποτελέσματα αποθαρρύνονται ή τιμωρούνται, από συγκεκριμένους μηχανισμούς αξιολόγησης και επιβράβευσης. Λειτουργούν θέτοντας τον αλγόριθμο να εργαστεί σε ένα περιβάλλον που σε κάθε επανάληψη το αποτέλεσμα ερμηνεύεται και αναλόγως ο αλγόριθμος επιβραβεύεται. Πιο κοινοί αλγόριθμοι σε αυτόν το τύπο μάθηση είναι οι Q-learning, Temporal difference (TD), Monte Carlo tree search (MCTS), Asynchronous actor-critic agents (A3C).
- Deep Learning: ανήκει στις τεχνικές της επιστήμη της μηχανικής μάθησης και συγκεκριμένα στα νευρωνικά δίκτυα που χρησιμοποιούν πολλαπλά επίπεδα για να εξάγουν υψηλού επιπέδου features των δεδομένων εισαγωγής και μπορεί να συνδυαστεί με οποιαδήποτε από τις προαναφερθείσες μεθόδους

μάθησης. Αποτελείται από τρία κύρια επίπεδα, τα input και hidden layers με σιγμοειδή συναρτήσεις και το output layer. Η ικανότητα τους αυξάνεται με την αύξηση του πλήθους των νευρώνων σε κάθε επίπεδο και του αριθμού των hidden layer. Η αύξηση αυτή όμως δημιουργεί απαιτήσεις σε μεγάλου πλήθους δείγματα και σε υψηλή υπολογιστική ισχύ. Μερικά διαδεδομένα μοντέλα είναι τα Recurrent neural networks (RNN) και η Long short-term memory (LSTM).



Εικόνα 33 Είδος μάθησης και μοντέλα ανά περίπτωση [55]

Τα ευφυή και συνδεδεμένα οχήματα παράγουν τεράστιες ποσότητες λειτουργικών και διαγνωστικών δεδομένων και ένα κλασσικό σύστημα κυβερνοασφάλειας δεν μπορεί αποδοτικά να αναγνωρίσει όλους τους εσωτερικούς κινδύνους που μπορεί να εγκυμονούν. Η μηχανική μάθηση μπορεί να προσφέρει λύσεις υψηλής ακρίβειας και πραγματικού χρόνου εντοπίζοντας ανωμαλίες και μοτίβα στα δεδομένα. Οι λύσεις της μπορούν να χρησιμοποιηθούν στο εσωτερικό δίκτυο του οχήματος (Vehicle Network), στην επίγνωση της κατάστασης του οχήματος (Situational Awareness) αλλά και στην νοημοσύνη του (Vehicle Intelligence). Διαφορετικά είδη μάθησης, οδηγούν στην επιλογή κατάλληλων αλγορίθμων με βασικό άξονα πάντα το αντικείμενο εφαρμογής. Ένα σύστημα IDS για το την ασφάλεια του εσωτερικό δίκτυο επικοινωνίας ενός ευφυούς και συνδεδεμένου οχήματος μπορεί να υποστηριχθεί και από τις πέντε κατηγορίες μάθησης (**Εικόνα 34**).



Εικόνα 34 Τομείς υποστήριξης της ανάπτυξης ασφαλών ICV βάση του τύπου της μάθησης

Κεφάλαιο 5 Υλοποίηση Προσομοίωσης

5.1 Απαιτήσεις και Σχεδιασμός

Προκειμένου να σχεδιαστεί και να δοκιμαστεί ένα εργαλείο ικανό να ανιχνεύει επιθέσεις στο πρωτόκολλο FlexRay είναι απαραίτητη η προετοιμασία ενός κατάλληλου περιβάλλοντος προσομοίωσης και ελέγχου. Η δημιουργία επικοινωνίας ανάμεσα σε δύο στοιχεία με το συγκεκριμένο πρωτόκολλο, απαιτεί την ύπαρξη κατάλληλου υλικού και πιο συγκεκριμένα, τουλάχιστον δύο transceivers και ένα κανάλι FlexRay. Στα πλαίσια της παρούσας διπλωματικής εργασίας, η πρόσβαση και διάθεση τέτοιου υλικού ήταν αδύνατη και σε συνδυασμό με την έλλειψη ελεύθερης διάθεσης τέτοιων λογισμικών και περιβαλλόντων στο εμπόριο, αποτέλεσε μια επιπλέον πρόκληση.

Η εκπόνηση της εργασίας, λοιπόν, αποφασιστικέ να αποτελείται από μια σειρά μεθοδικών υλοποιήσεων συγκεκριμένων λογισμικών και λειτουργιών. Πιο συγκεκριμένα, αρχικά είναι απαραίτητος ο σχεδιασμός και η υλοποίηση ενός λογισμικού κατάλληλου για την προσομοίωση της επικοινωνίας FlexRay ανάμεσα σε δύο κόμβους. Για τον σκοπό αυτόν, αναπτύχθηκε το λογισμικό *FlexRayGen*, το οποίο δημιουργεί την επικοινωνία πάνω στο δίκτυο. Κατόπιν, προκειμένου να υπάρχει παρακολούθηση και μελέτη της επικοινωνίας, προγραμματίστηκε το λογισμικό *FlexRayShark*, το οποίο παρακολουθεί την επικοινωνία που δημιουργεί το FlexRayGen, και προβάλει στον χρήστη όλη την πληροφορία των πακέτων που ανταλλάσσονται. Η ανίχνευση επιθέσεων απαιτεί πρωτίστως την ύπαρξη τους, οπότε το επόμενο στάδιο είναι φυσικά η εφαρμογή συγκεκριμένων επιθέσεων πάνω στο περιβάλλον εργασίας, μέσω του πρώτου προγράμματος. Τέλος ο σχεδιασμός της ανίχνευσης απαιτεί η συλλογή των δεδομένων της επικοινωνίας από το λογισμικό FlexRayShark και κατόπιν την ανάπτυξη και επαλήθευση των αλγορίθμων με εκτέλεση συγκεκριμένων πειραμάτων.

5.2 Παραδοχές

Οι απαιτήσεις και οι διαθέσιμοι πόροι, οδήγησαν στις παρακάτω παραδοχές για την εκπόνηση της μελέτης:

- Ο μηχανισμός πίσω από τις προσομοιωμένες επιθέσεις ισοδυναμεί είτε με φυσική πρόσβαση στο μέσο είτε με κακόβουλο λογισμικό που έχει προσβάλει έναν από τους δύο κόμβους είτε φυσικά με δράση πρόσθετου υλικό στο μέσο ή τον κόμβο.
- Υλοποιήθηκαν μόνο οι απαραίτητοι μηχανισμοί του πρωτοκόλλου προκειμένου να ανταποκρίνεται στις απαιτήσεις και τις προδιαγραφές που αναλύθηκαν προηγουμένως. Πιο συγκεκριμένα υποστηρίζεται επικοινωνία στο στατικό τμήμα του κύκλου επικοινωνίας και παραλείπονται διαδικασίες εκκίνησης της. Χρησιμοποιείται ένα κανάλι και δύο κόμβοι FlexRay.
- Οι επιθέσεις είναι πλήρως επιτυχημένες και δύσκολα ανιχνεύσιμες. Εκτελούνται στους σωστούς χρόνους, στις σωστές χρονοθυρίδες, τηρώντας τις συχνότητες και ακολουθώντας τις φάσεις του κύκλου επικοινωνίας. Πρόκειται για ένα ιδιαίτερα δύσκολο σενάριο στο οποίο ο επιτιθέμενος είναι απαραίτητο να έχει σχεδόν πλήρη γνώση της αρχιτεκτονικής και των παραμέτρων της υπό στόχευση τοπολογίας FlexRay. Θεωρείται πως η ανίχνευση σε φυσικό επίπεδο δεν ήταν επιτυχής και εξετάζεται η αποδοτικότητα της στο επόμενο επίπεδο, αυτό της διασύνδεσης των δεδομένων.

5.3 Σχετικές Εργασίες

Οι συγγραφείς του *"AI-Based Intrusion Detection Systems for In-Vehicle Networks "* [11] κατηγοριοποιούν τα διαθέσιμα μοντέλα μηχανικής μάθησης για τον σχεδιασμό ενός Intrusion Detection System και δοκιμάζουν πολλαπλούς αλγορίθμους στο CAN πρωτόκολλο, μεταξύ των οποίων και τα SVM, kNN, RF και LSTM. Ολοκληρώνοντας στις προτάσεις τους αναδεικνύουν την έλλειψη σε datasets, την αδυναμία σε ανίχνευση χαμηλής συχνότητας επιθέσεων και τον κίνδυνο που εγκυμονεί για τα συστήματα ανίχνευσης. Ομοίως ο Ajeet Kumar Dwivedi [18] δοκιμάζει επιπλέον τα μοντέλα Logistic Regression, SVC, Xgboost, FFNN προτείνοντας τον σχεδιασμό ενός Anomaly Based IDS σε CAN. Την μελέτη τους σε CAN επικεντρώνουν και οι B.S.Bari, K.Yelamarthi και S.Ghafoor [17] με στόχο την ανίχνευση επιθέσεων όπως DoS, fuzzy, impersonation, flooding και malfunction εστιάζοντας στην μηχανική μάθηση για τον σχεδιασμό ενός IDS. Χρησιμοποιούν τα μοντέλα kNN , SVM και Decision Trees

καταλήγοντας σε πολύ ικανοποιητικά αποτελέσματα, υπογραμμίζοντας όμως την ανάγκη για datasets.

Ο Nevrus Kaja [15] στην ντοκτορά του σχετικά με την ασφάλεια του V2X δικτύου, παρουσιάζει τους μηχανισμούς ανίχνευσης και δημιουργεί ένα περιβάλλον τριών βημάτων για την ανίχνευση απειλών χρησιμοποιώντας αλγορίθμους μηχανικής μάθησης συμπεριλαμβανομένων των SVM και Random Forest. Το Intrusion Detection System προτείνει αποδίδει εξαιρετικά τονίζοντας όμως την ανάγκη για datasets και επιλογή μοντέλων βάσει των χαρακτηριστικών του υπό μελέτη συστήματος και όχι των επιδόσεων.

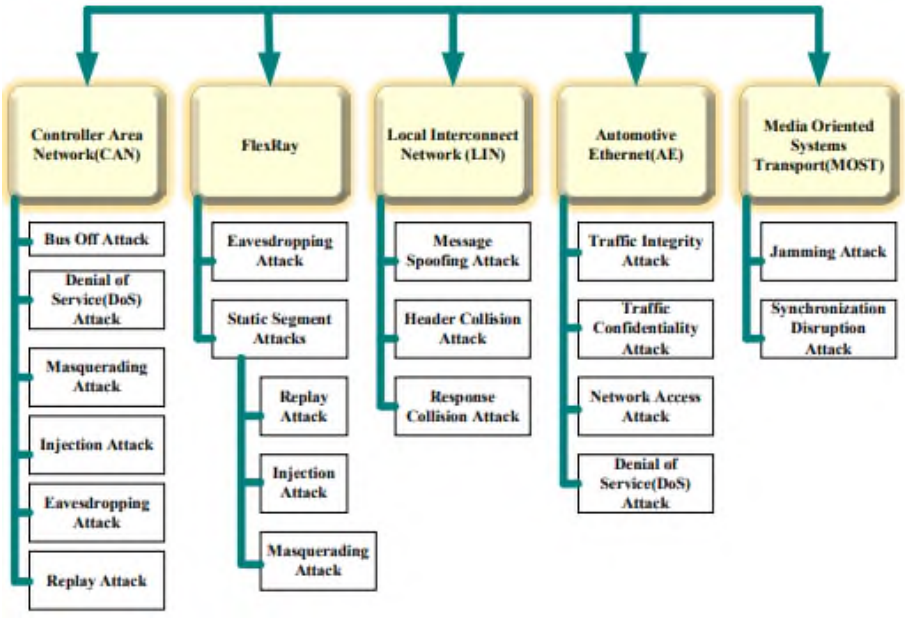
Στο άρθρο "*Intrusion Detection and Prevention System for FlexRay against Spoofed Frame Injection*" [47], παρουσιάζεται η ευπάθεια του πρωτοκόλλου FlexRay στις spoofed frame επιθέσεις και προτείνεται ένα Intrusion Detection and Prevention System για την ανίχνευση τους στο φυσικό επίπεδο. Οι Pal Stefan Murvay και Bogdan Groza [8] εκτός από τις spoofing επιθέσεις επικεντρώνονται στις DoS εκτελώντας πειράματα στο φυσικό επίπεδο με πραγματικούς transceiver και δοκιμάζοντας διάφορες τοπολογίες. Η SAE International στο άρθρο της "*Vulnerability of FlexRay and Countermeasures*" [7] παρουσιάζει τις ευπάθειες του FlexRay μέσω πειραμάτων στο φυσικό επίπεδο και προτείνει συγκεκριμένες λύσεις, υπογραμμίζοντας την ανάγκη για περισσότερη έρευνα στην ανίχνευση και στην ανταπόκριση σε αυτήν. Στην ανασκόπηση τους ο Narayan Kharti και συν. [70] παροτρύνουν την επιστημονική κοινότητα να εστιάσει στην συλλογή labeled datasets, στην σχεδίαση μηχανισμών άμυνας πολλών επιπέδων και όχι μόνο στο physical και application layer, στην μελέτη πολλών περισσοτέρων επιθέσεων και στην μείωση της πολυπλοκότητας των μεθόδων IDS.

Εν κατακλείδι η βιβλιογραφία είναι ως επί των πλείστων αφιερωμένη σε μηχανισμούς στο φυσικό επίπεδο, με πολλά πειράματα και αποτελέσματα σε πραγματικά οχήματα. Εκλείπει η εμφάνιση του πρωτοκόλλου FlexRay ενώ υπάρχουν αρκετές διαθέσιμες μελέτες για το CAN. Ταυτόχρονα οι περισσότερες προτεινόμενες λύσεις είναι αφιερωμένες σε μοντέλα που στηρίζονται σε αλγορίθμους μηχανικής μάθησης και σχεδιασμό Intrusion Detection Systems. Κοινή αποδοχή όλων όμως αποτελεί η

έλλειψη σε διαθέσιμα δεδομένα προς μελέτη ενώ η διακρίνεται και η ανάγκη για ανίχνευση και σε άλλα επίπεδα του δικτύου.

5.4 Επιλογή Επιθέσεων και Μηχανισμών Ανίχνευσης

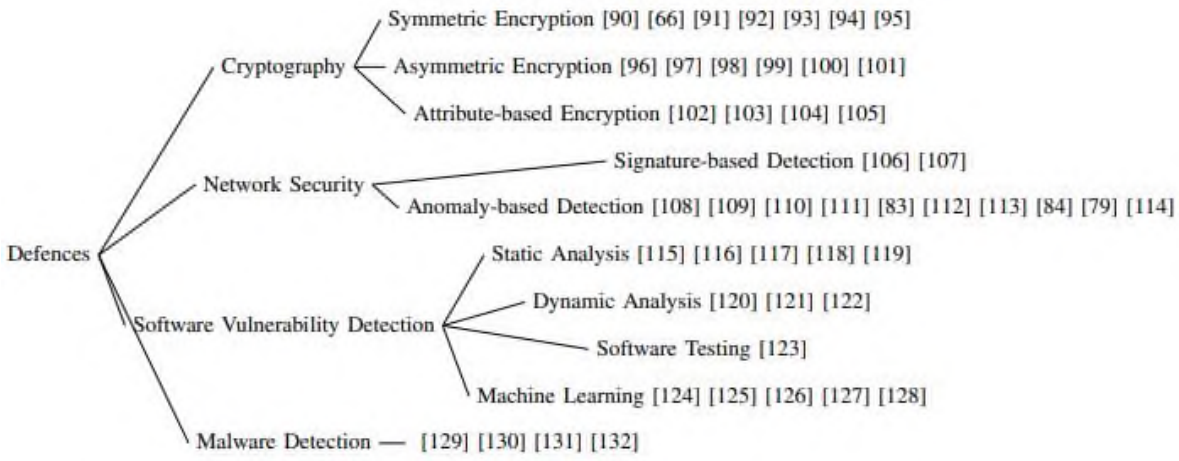
Οι δύο επιθέσεις που αποφασίστηκε να μελετηθούν είναι η επανάληψη και η έγχυση μηνύματος για δύο λόγους. Πρώτον, σύμφωνα με το άρθρο "*In-Vehicle Communication Cyber Security: Challenges and Solutions*" [25] (**Εικόνα 35**), που κάνει μια ταξινόμηση των επιθέσεων βάσει του πρωτοκόλλου επικοινωνίας, αποτελούν δύο από τις κυριότερες επιθέσεις στο στατικό τμήμα του FlexRay.



Εικόνα 35 Ταξινόμηση επιθέσεων ανά πρωτόκολλο ενδοεπικοινωνίας [25]

Δεύτερον και οι δύο εμφανίζονται αρκετά στην βιβλιογραφία ([8], [12], [14], [15], [16]) με την επανάληψη μηνύματος όμως να μελετάται περισσότερο στο φυσικό επίπεδο από ότι η έγχυση.

Η ανάπτυξη ενός τέτοιου εργαλείου, που θα μελετά την κατάσταση του οχήματος και θα αξιολογεί τα δεδομένα προκειμένου να διαπιστώσει κακόβουλες ενέργειες, θα πρέπει να κινηθεί είτε στην ανίχνευση ανωμαλιών είτε στην ανίχνευση βασισμένη στην υπογραφή (**Εικόνα 36**), σύμφωνα και με το άρθρο "*An Overview of Attacks and Defends on Intelligent Connected Vehicles* " [12], στο οποίο γίνεται μια ταξινόμηση των τύπων των επιθέσεων και των μηχανισμών επιθέσεων.



Εικόνα 36 Ταξινόμηση μηχανισμών άμυνας [12]

Οι επιθέσεις που εξετάζονται στην παρούσα εργασία ταξινομούνται στο επίπεδο της ασφάλειας δικτύου, οπότε η εργασία προσανατολίστηκε σε αλγορίθμους ανίχνευσης ανωμαλιών, στο επίπεδο διασύνδεσής των δεδομένων του πρωτοκόλλου FlexRay [14]. Οι αλγόριθμοι που επιλέχθηκαν για τον σκοπό αυτόν ήταν ένα μοντέλο διανυσματικής υποστήριξης ταξινόμησης (Support Vector Classification), ένα νευρωνικό δίκτυο εμπρόσθιας τροφοδοσίας (Feed Forward Neural Network), ένα μοντέλο των k εγγύτερων γειτόνων (k Nearest Neighbors), ένα Random Forest και η Long Short-Tern Memory. Οι λόγοι που οδήγησαν στην επιλογή αυτή ήταν αρχικά η ανάγκη για ποικιλία και δοκιμή. Σε τέτοιες μελέτες είναι απαραίτητο να δοκιμάζονται και να καταγράφονται τα αποτελέσματα της απόδοσης πολλών διαφορετικών μοντέλων προκειμένου να βγουν συμπεράσματα και να επιλεγούν τα κατάλληλα. Κατά δεύτερον υπήρχε η ανάγκη ελέγχου της time-based ανίχνευσης, της payload-based και φυσικά του συνδυασμού τους μέσω της υβριδικής, οπότε τα μοντέλα έπρεπε να μπορούν να ανταποκριθούν τουλάχιστον σε μια από αυτές. Τέλος η επιλογή τους έπρεπε να συνάδει με την βιβλιογραφία. Και τα πέντε μοντέλα εμφανίζονται σε αρκετά πειράματα και μελέτες τόσο για την δοκιμή τους όσο και για την πρόταση του σε συστήματα ανίχνευσης ([11], [15], [17], [18], [12]).

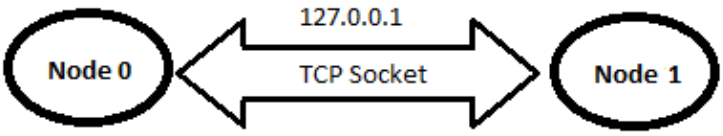
5.5 Λογισμικό FlexRayGen

Το FlexRayGen είναι υπεύθυνο για την προσομοίωση της επικοινωνίας και των επιθέσεων. Δημιουργεί δύο κόμβους FlexRay που επικοινωνούν μεταξύ τους βάσει ενός προσχεδιασμένου σχήματος δέσμευσης χρονοθυρίδων. Όλες οι παράμετροι του

πρωτοκόλλου είναι παραμετρικοποιήσιμες, με ονόματα που συμφωνούν με τις αντίστοιχες μεταβλητές που ορίζονται στο έγγραφο προδιαγραφών [2]. Επίσης δημιουργεί τον επιτιθέμενο κόμβο, που παρεμβάλλεται ανάμεσα στους δύο επικοινωνούντες κόμβους ως Man in the Middle Attack (MitM).

5.5.1 Bus and Physical Layer

Το φυσικό επίπεδο είναι αδύνατο να υποστηριχθεί χωρίς το απαραίτητο υλικό και έτσι προσομοιώθηκε πάνω στο TCP πρωτόκολλο (**Εικόνα 37**). Το κανάλι Α, αντιστοιχεί σε ένα TCP socket που λειτουργεί στο loopback interface του δικτύου. Κάθε κόμβος δημιουργεί ένα socket descriptor ρυθμισμένο σε non-blocking λειτουργία και τον χρησιμοποιεί για να στέλνει και να λαμβάνει μηνύματα από τους κόμβους του cluster.

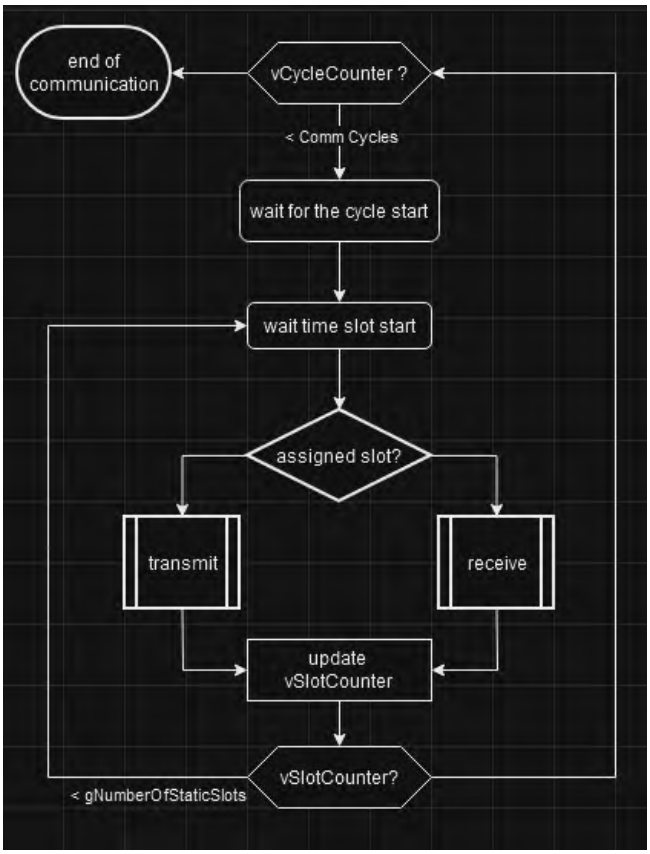


Εικόνα 37 Προσομοίωση φυσικού επιπέδου στο FlexRayGen

5.5.2 Communication Cycle

Οι παράμετροι της επικοινωνίας καθορίζονται από τον προγραμματιστή σε επίπεδο προεπεξεργαστή και μπορούν να προσδιοριστούν από το αρχείο "*flexray.hpp*". Κάθε κόμβος ορίζεται ως ένα αντικείμενο κλάσης FlexRayTrx και αποτελεί ένα νήμα. Μερικές από τις ιδιωτικές μεταβλητές του κόμβου είναι ένας αναγνωριστικός αριθμός, το πλήθος των πλαισίων που μεταδίδει ανά κύκλο, που ορίζεται σε 50% των συνολικών χρονοθυρίδων, η διάρκεια κάθε κύκλου και χρονοθυρίδας και φυσικά το σχήμα δέσμευσης των χρονοθυρίδων στο στατικό σχήμα. Ο κόμβος που ξεκινά πρώτος την επικοινωνία, καταγράφει την χρονική στιγμή εκκίνησης της και την αποθηκεύει σε μια global μεταβλητή. Η τιμή αυτή χρησιμοποιείται ως σημείο αναφοράς για τον συγχρονισμό των διαδικασιών των δύο νημάτων. Πριν την εκκίνηση όμως, προηγείται η εγκαθίδρυση του καναλιού Α, μέσω της tcp socket και της κλασσικής διαδικασίας server-client. Η IP διεύθυνση για tcp socket σε loopback interface έχει γνωστή τιμή 127.0.0.1 και το μόνο που καθορίζεται είναι η θύρα του

server κόμβου. Στην **Εικόνα 38**, παρουσιάζεται το διάγραμμα ροής μιας επικοινωνίας με καθορισμένο πλήθος κύκλων εκτέλεσης.



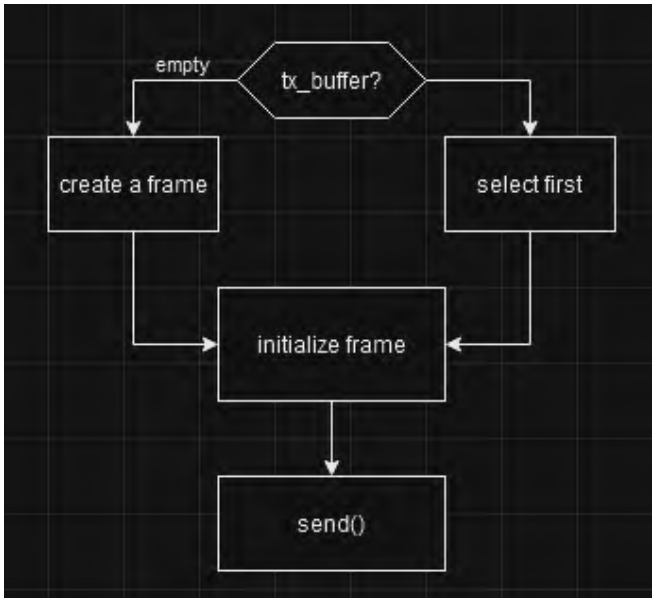
Εικόνα 38 Διάγραμμα ροής ρουτίνας κάθε κόμβου

Κάθε κόμβος υπολογίζει την χρονική στιγμή εκκίνησης του κύκλου, χρησιμοποιώντας σαν σημείο αναφοράς την global μεταβλητή έναρξης της επικοινωνίας και περιμένει μέχρι αυτή να επέλθει. Αμέσως μετά αρχίζει την εκτέλεση του στατικού τμήματος, με την έναρξη της πρώτης χρονοθυρίδας. Όπως και στον κύκλο, κάθε κόμβος υπολογίζεται το σημείο εκκίνησης της χρονοθυρίδας (action point) και αναμένει μέχρι τον ερχομό της. Στο διάγραμμα δεν διακρίνεται άμεσα η αναμονή κατά το idle segment του κύκλου καθώς αυτό επιτυγχάνεται έμμεσα μέσω των αναμονών και συγχρονισμό, τηρώντας όμως το σχήμα του πρωτοκόλλου.

5.5.3 Transmission and Reception

Σύμφωνα με το σχήμα του κύκλου επικοινωνίας σε κάθε χρονοθυρίδα ένας κόμβος μπορεί είτε να μεταδώσει είτε να λάβει FlexRay πλαίσια. Μετάδοση μπορεί να πραγματοποιηθεί αποκλειστικά και μόνο από τον κόμβο για τον οποίο έχει δεσμευτεί

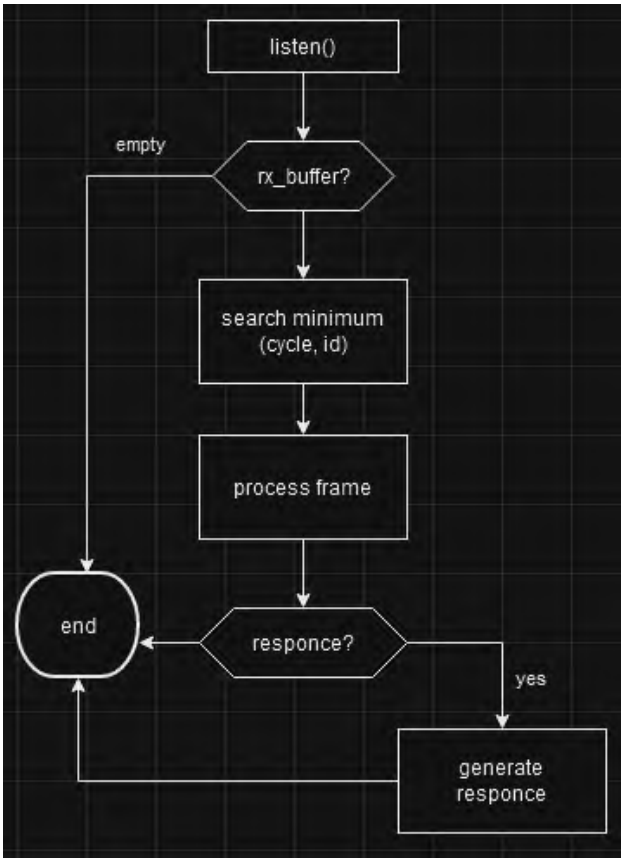
η χρονοθυρίδα. Στην **Εικόνα 39**, παρουσιάζεται το διάγραμμα ροής της μεθόδου μετάδοσης του αντικειμένου κόμβου. Κάθε κόμβος διαθέτει ένα χώρο διατήρησης πλαισίων, tx_buffer, για την αποθήκευση αυτών που γεννώνται ως αποκρίσεις σε λαμβάνονται πλαίσια. Αν ο χώρος αυτός είναι άδειος παράγει ένα πλαίσιο, αλλιώς επιλέγει το πρώτο διαθέσιμο. Κατόπιν το αρχικοποιεί, μια διαδικασία που αποτελείται από τον καθορισμό των μεταβλητών αναγνωριστικού πλαισίου και μετρητή κύκλου, πεδία frame id και cycleCount αντίστοιχα, και το μεταδίδει στο κανάλι Α.



Εικόνα 39 Διάγραμμα ροής διαδικασίας μετάδοσης κόμβου

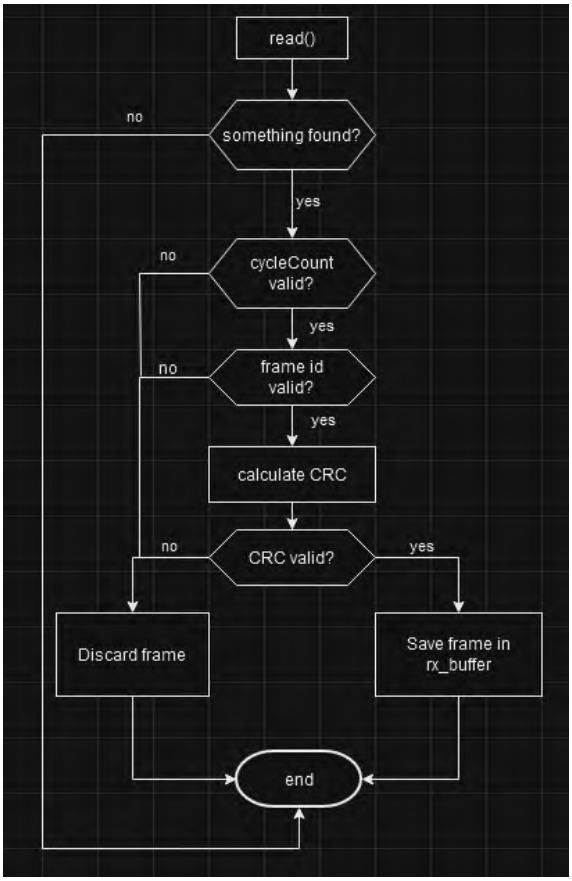
Στην περίπτωση που η χρονοθυρίδα δεν ανήκει στο κόμβο (**Εικόνα 38**), τότε επιλέγει να ακούσει το κανάλι και στην συνέχεια να προχωρήσει σε επεξεργασία. Για τον σκοπό αυτό κάθε κόμβος εκτός από τον χώρο αποθήκευσης πλαισίων προς μετάδοση διαθέτει και τον χώρο αποθήκευσης πλαισίων λήψης, rx_buffer, στον οποίο διατηρεί ότι έχει αναγνώσει από το κανάλι και δεν επεξεργάστηκε ακόμα.

Η διαδικασία της επεξεργασίας αποτελείται από τον έλεγχο της ομοιότητας του μετρητή κύκλου που φέρει το πλαίσιο με αυτόν που διαθέτει ο κόμβος και κατόπιν την επεξεργασία του. Η επιλογή παραγωγής απόκρισης για το ληφθέν πλαίσιο στηρίζεται σε τυχαίο παράγοντα. Η διαδικασία παρακολούθησης του καναλιού, listen, περιγράφεται από το διάγραμμα ροής στην **Εικόνα 40**.



Εικόνα 40 Διάγραμμα ροής διαδικασίας ανάγνωσης του καναλιού

Στην περίπτωση που διαβάσει κάποιο πλαίσιο από το κανάλι (**Εικόνα 41**), ελέγχει το μετρητή κύκλου και το αναγνωριστικού πλαισίου για εγκυρότητα, συγκρίνοντας τα με τους δικούς μετρητές. Σε περίπτωση εγκυρότητας προχωρά στον υπολογισμό και τον έλεγχο του κυκλικού ελέγχου πλεονασμού (CRC) και αν και αυτός συμφωνεί τότε το πλαίσιο είναι έγκυρο και αποθηκεύεται στο rx_buffer. Σε περίπτωση σφάλματος εγκυρότητας το πλαίσιο απορρίπτεται, ενώ σε κάθε άλλη περίπτωση η διαδικασία τερματίζεται.



Εικόνα 41 Διάγραμμα ροής της διαδικασίας λήψης του κόμβου

5.5.4 Δημιουργία Πλαισίου

Το πλαίσιο ορίζεται ως μια δομή μεταβλητών, όπως φαίνεται στην **Εικόνα 42**. Κάθε μεταβλητή είναι ένα πεδίο του FlexRay πλαισίου.

```
struct frame_t
{
    /* Header Segment */
    uint8_t reserved   :1;  // reserved
    uint8_t payId      :1;  // payload preamble indicator
    uint8_t null_frame :1;  // null frame indicator
    uint8_t sync       :1;  // sync frame indicator
    uint8_t start_up   :1;  // start up frame indicator
    uint16_t frame_id  :11; // frame id
    uint8_t length     :7;  // length
        uint16_t h_crc     :11; // Header CRC
        uint8_t cycleCount :6;  // cycle count
    /* Payload Segment */
        char payload[255];         // 254 Bytes + '\0'
        /* Trailer Segment */
    uint8_t crc0;
    uint8_t crc1;
    uint8_t crc2;
};
```

Εικόνα 42 Ορισμός δομής προσομοίωσης του FlexRay πλαισίου

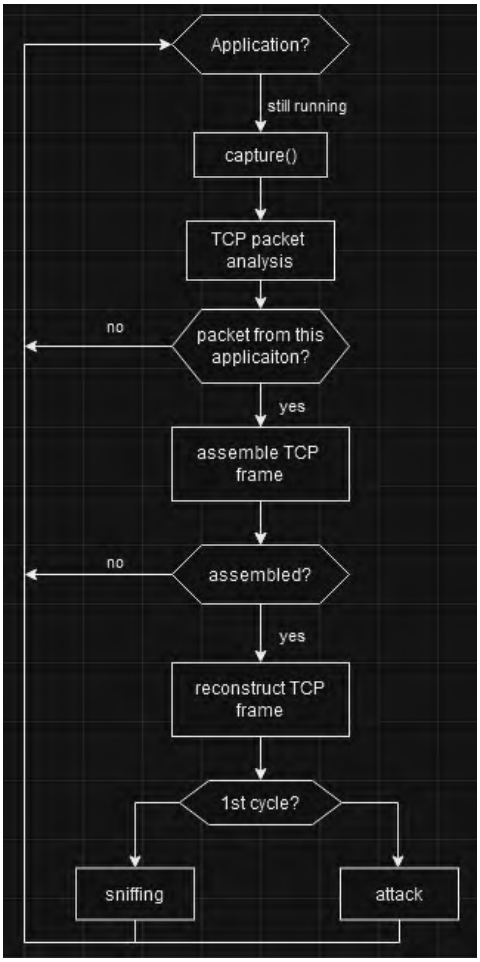
Η διαδικασία της δημιουργίας ενός πλαισίου είναι αρκετά ντετερμινιστική και περιορίζεται από τις λειτουργίες του πρωτοκόλλου που επιλέχθηκαν να υλοποιηθούν. Ξεκινώντας με το τμήμα της κεφαλής, τα πεδία αρχικοποιούνται σύμφωνα με τις οδηγίες προκειμένου να αποτελέσουν πλαίσια στατικού τμήματος. Το τμήμα των δεδομένων τίθεται κάθε φορά ολόκληρο με τυχαίο τρόπο, μέσα από μια συλλογή πεζών και κεφαλαίων χαρακτήρων αλλά και αριθμών. Οι κυκλικοί έλεγχοι πλεονασμού, το αναγνωριστικό πλαισίου και ο μετρητής κύκλου καθορίζονται στην διαδικασία της μετάδοσης, κατά την αρχικοποίηση του πλαισίου μετάδοσης. Για τον υπολογισμό των CRC των 24 bit για το τμήμα ουράς και 11 bit για το αντίστοιχο πεδίο του τμήματος κεφαλής, ακολουθήθηκαν οι αλγόριθμοι του Markus Iversen Huse [1] με τις τιμές και τις παραμέτρους να λαμβάνονται σύμφωνα με το έγγραφο προδιαγραφών του πρωτοκόλλου [2].

5.5.5 Νήμα Raptor

Για την εφαρμογή των επιθέσεων και την παρακολούθηση της επικοινωνίας των δύο προαναφερθέντων κόμβων, δημιουργείται ένα επιπλέον νήμα, με το όνομα Raptor, το οποίο λειτουργεί ως Man-in-the-Middle-Attack.

5.5.5.1 Σύλληψη πακέτων

Χρησιμοποιώντας την pcap βιβλιοθήκη της C++ ανοίγει την διεπαφή loopback του δικτύου και πιάνει όλα τα πακέτα που κινούνται σε αυτήν, σένα πιθανό εύρος θυρών. Το εύρος χρησιμοποιείται διότι, παρότι η θύρα του κόμβου-διακομιστή είναι γνωστή, η θύρα του κόμβου-πελάτη δεν είναι προκαθορισμένη. Από την στιγμή που το κανάλι Α προσομοιώνεται σε TCP socket, η θύρα προορισμού και προέλευσης κάθε πακέτου μπορεί να εντοπιστεί και έτσι, γνωρίζοντας μόνο μια εκ των δύο κόμβων θύρα, μπορεί να αποφασιστεί αν το πακέτο αφορά την επικοινωνία ή προέρχεται από άλλη εφαρμογή. Παρακάτω φαίνεται το συνοπτικό διάγραμμα ροής του νήματος (**Εικόνα 43**).



Εικόνα 43 Διάγραμμα ροής της σύλληψης των πλαισίων από τον Raptor

Όσο δεν έχει ζητηθεί τερματισμός της εφαρμογής το νήμα πιάνει όσα πακέτα βρίσκει στην διεπαφή και τα αναλύει ως TCP πακέτα. Για κάθε ένα από αυτά ελέγχει με τον τρόπο που περιγράφηκε προηγουμένως αν αποτελεί πακέτο ενδιαφέροντος ή όχι. Στη περίπτωση που αποτελεί, προσπαθεί να το συναρμολογήσει λαμβάνοντας υπόψιν όλα όσα έλαβε πριν από αυτό και δεν τα έχει συναρμολογήσει ακόμα. Μόλις τα καταφέρει τότε δημιούργησε ένα FlexRay πλαίσιο. Στην περίπτωση που η επικοινωνία βρίσκεται στον πρώτο κύκλο, τότε απλώς παρακολουθεί την εξέλιξη της και καταγράφει τα χαρακτηριστικά γνωρίσματά της. Μέσα σε αυτά περιλαμβάνονται το πλήθος των χρονοθυρίδων και το σχήμα ανάθεσης τους στους δύο κόμβους. Για κάθε άλλο κύκλο, το νήμα εφαρμόζει την επίθεση που επέλεξε ο χρήστης από τη διεπαφή της εφαρμογής.

5.5.5.2 Επίθεση Επανάληψης Μηνύματος

Γνωστή ως Message Replay, περιλαμβάνει την σύλληψη ενός μηνύματος κατά την διάρκεια μια επικοινωνίας και την επαναλαμβανόμενη μετάδοση του προς ένα ή πολλαπλούς προορισμούς στο δίκτυο. Στόχος της επίθεσης είναι συνήθως να οδηγήσει το σύστημα στην συνεχή λήψη των συγκεκριμένων πακέτων ώστε να αγνοήσει και να μην λάβει τα μηνύματα της αυθεντικής πηγής. Για την εφαρμογή της επίθεσης από τον Raptor, αρχικά είναι απαραίτητη η δημιουργία του μηνύματος επανάληψης. Αυτό επιλέγεται τυχαία κατά την παρακολούθηση του πρώτου κύκλου επικοινωνίας. Κατόπιν σε κάθε επόμενο κύκλο και σε κάθε επόμενη χρονοθυρίδα του κόμβου-διακομιστή ο Raptor μεταδίδει αυτό το πλαίσιο. Αποτέλεσμα ο κόμβος-πελάτης να λαμβάνει αποκλειστικά και μόνο το ίδιο πακέτο, μέχρι και την ολοκλήρωση όλων των κύκλων επικοινωνίας. Φυσικά προκειμένου να επιτευχθεί αυτό ο Raptor πριν την μετάδοση ενημερώνει το αναγνωριστικό πλαισίου και τον μετρητή κύκλου, καθώς επίσης επανυπολογίζει τα αριθμούς κυκλικού ελέγχου πλεονασμού τόσο για το τμήμα κεφαλής όσο και για το τμήμα ουράς.

5.5.5.3 Επίθεση Έγχυσης Μηνύματος

Γνωστή ως Message Injection, αφορά στην εισαγωγή ενός κακόβουλου μηνύματος στο μέσο επικοινωνίας. Καθώς δύο μέρη επικοινωνούν ένας εξωτερικός παράγοντας, παρεμβάλλεται και εγχύει στο δίκτυο το μήνυμα, με αποτέλεσμα να το λαμβάνει ο παραλήπτης και συνήθως να αγνοεί το αυθεντικό. Για την επίτευξη αυτού του σκοπού ο Raptor πρέπει να περιμένει την κατάλληλη χρονοθυρίδα και να ενθέσει το δικό του. Σε αντίθεση με την επίθεση επανάληψης μηνύματος, στην περίπτωση αυτή το δίκτυο δεν προσβάλλεται σε κάθε χρονοθυρίδα καθενός κύκλου, αλλά σε επιλεγμένα σημεία και στιγμές. Η επιλογή αυτών των στιγμών είναι τυχαίες και σχετικά συχνές, προκειμένου να αποδώσουν ιδανικά. Φυσικά πριν την μετάδοση οποιουδήποτε πλαισίου, πραγματοποιείται ενημέρωση των μετρητών και αρχικοποίηση των πεδίων αυτού. Και αυτή η επίθεση γίνεται στα μεταδιδόμενα μηνύματα του κόμβου-διακομιστή.

5.6 Λογισμικό FlexRayShark

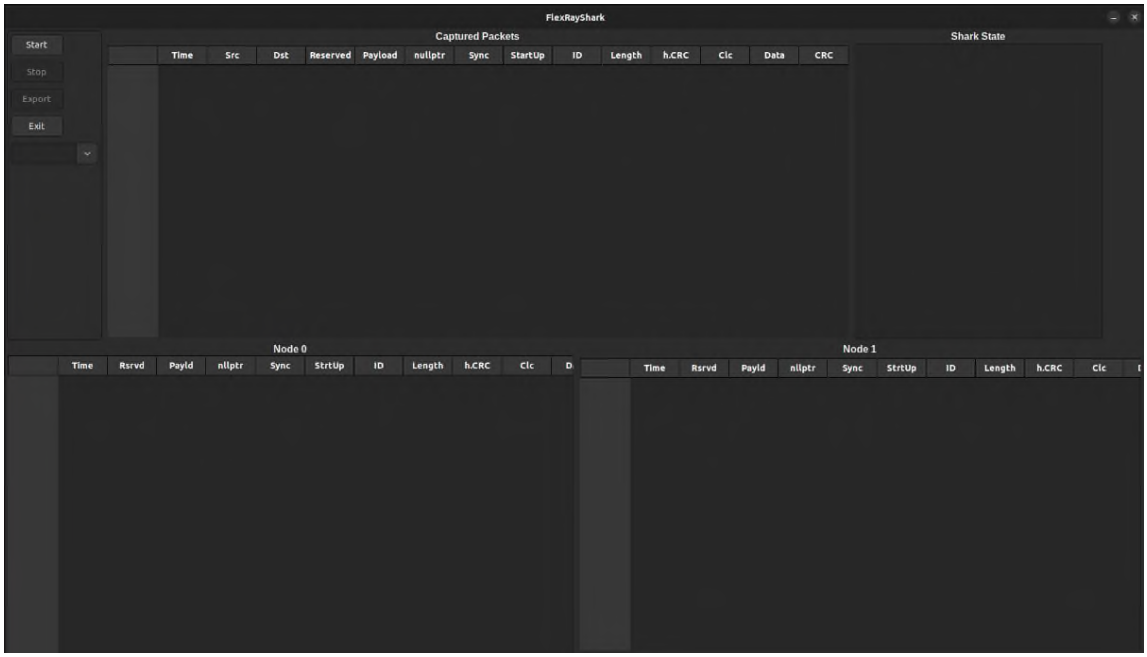
Σκοπός του λογισμικού αυτού είναι η διάδραση του χρήστη με το λογισμικό FlexRayGen. Πιο συγκεκριμένα αποτελεί την γραφική διεπαφή μέσω της οποίας ο

χρήστης μπορεί να επιλέξει πότε και με ποιες παραμέτρους επιθυμεί να εκτελέσει τον προσομοιωτή, αλλά και να έχει πλήρη εικόνα όλης της εξέλιξης και των γεγονότων που συμβαίνουν στην διάρκεια αυτής. Τα δύο λογισμικά επικοινωνούν άμεσα μέσω ενός pipe όπως θα αναλυθεί και παρακάτω. Τέλος σημειώνεται πως για την την γραφική απεικόνιση χρησιμοποιήθηκε η βιβλιοθήκη wxWidgets για C++.

5.6.1 Γραφική Σχεδίαση και Σενάρια Χρήσης

5.6.1.1 Αρχική Οθόνη και Επιλογές

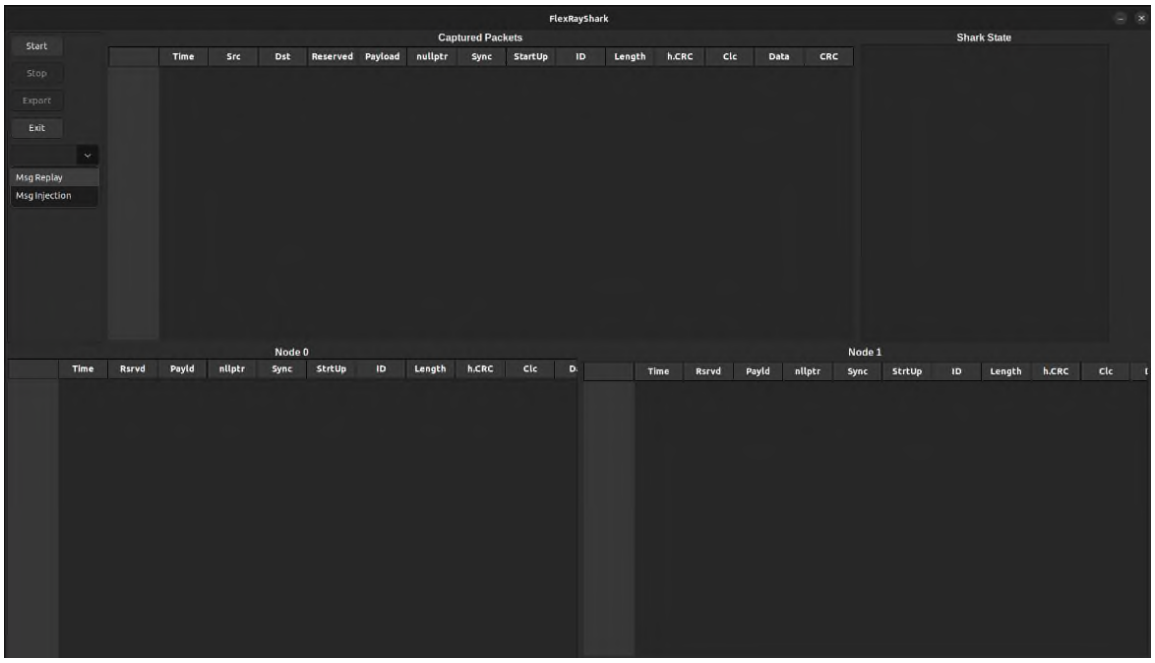
Μόλις εκτελεστεί το FlexRayShark, ανοίγει το αρχικό παράθυρο (**Εικόνα 44**).



Εικόνα 44 Στιγμιότυπο της αρχικής οθόνης της εφαρμογής FlexRayShark

Σε αυτό απεικονίζονται τέσσερα κουμπιά στην αριστερή πάνω πλευρά και τρία πλέγματα, ένα στο κέντρο πάνω και δύο αριστερά κάτω και δεξιά κάτω. Στην πάνω δεξιά γωνία βρίσκεται ένα πλαίσιο κειμένου. Αρχικά παρατηρείται πως τα κουμπιά “Stop” και “Export” είναι απενεργοποιημένα και το πλαίσιο κειμένου, όπως και τα πλέγματα άδεια. Αυτό οφείλεται στο γεγονός πως έχει ανοίξει μόνο το γραφικό περιβάλλον και δεν έχει ξεκινήσει ούτε το FlexRayGen ούτε οι υπηρεσίες του FlexRayShark. Κατά συνέπεια, στην φάση αυτή ο χρήστης μπορεί να επιλέξει είτε το κουμπί “Start” και να ξεκινήσει την προσομοιώση, είτε να κλείσει την εφαρμογή επιλέγοντας είτε το “Exit” είναι το ‘x’ του παραθύρου πάνω δεξιά. Όπως παρουσιάστηκε στην προηγούμενη ενότητα, το λογισμικό προσομοίωσης

υποστηρίζει επιθέσεις επανάληψης και επιθέσεις έγχυσης πλαισίου. Η επιλογή αυτή είναι δυνατόν να προσδιοριστεί πριν την εκκίνηση της εφαρμογής, από το πλαίσιο επιλογών που βρίσκεται κάτω από τα διαθέσιμα κουμπιά (**Εικόνα 45**).

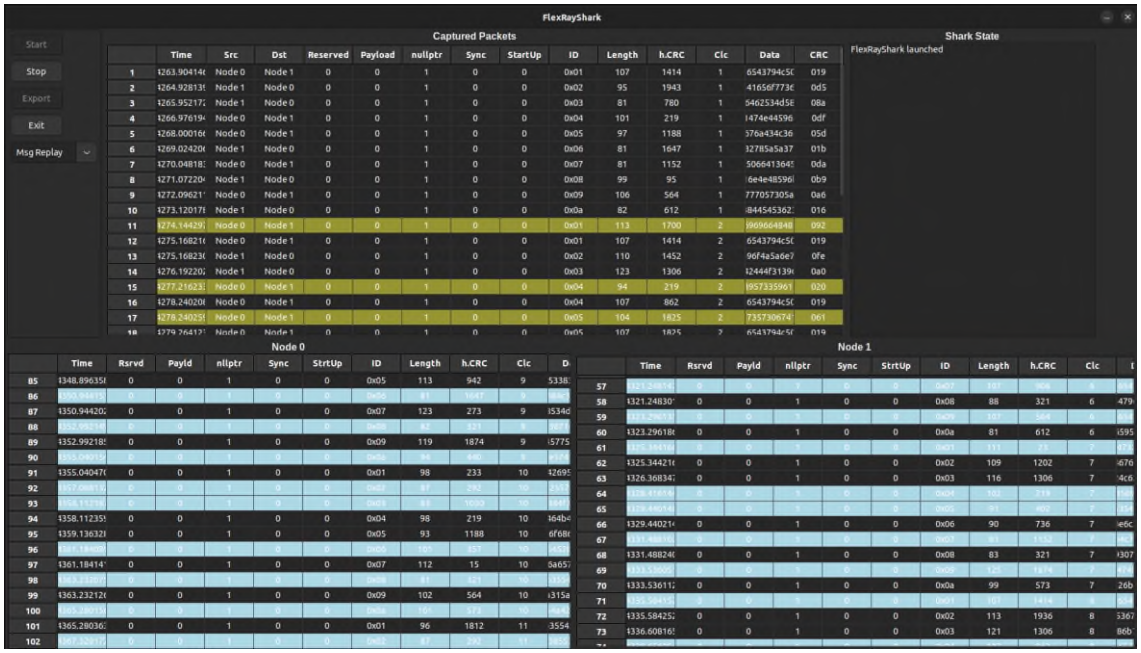


Εικόνα 45 Στιγμιότυπο του πλαισίου επιλογή επίθεσης

Στην περίπτωση που δεν επιλεγεί τύπος επίθεσης, το λογισμικό FlexRayGen δεν εφαρμόζει επιθέσεις και εκτελεί μια αυθεντική επικοινωνία ανάμεσα στους κόμβους.

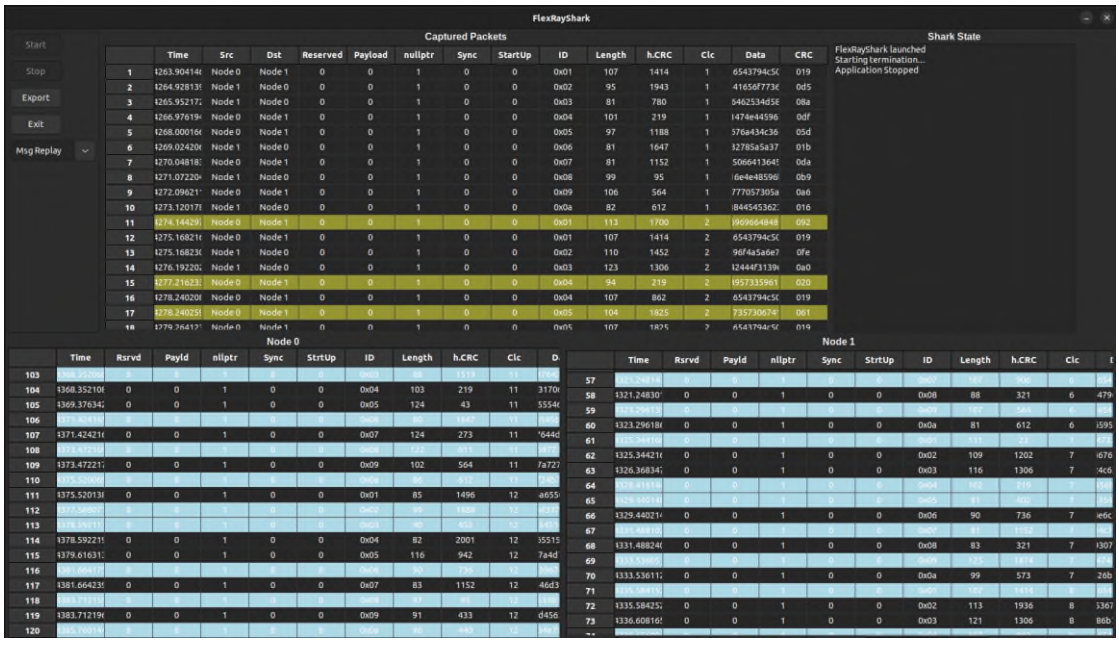
5.6.1.2 Κουμπιά Εκκίνησης, Διακοπής και Εξαγωγής

Μόλις ο χρήστης έχει αποφασίσει αν επιθυμεί μια αυθεντική ή μια προσβεβλημένη επικοινωνία, μπορεί να επιλέξει το κουμπί “Start” (**Εικόνα 46**). Αμέσως, όπως απεικονίζεται στην εικόνα , τα πλέγματα αρχίζουν να γεμίζουν με δεδομένα και στο πλαίσιο κειμένου γίνεται ενημέρωση πως η εφαρμογή προσομοίωσης εκκινήθηκε. Η σημασία των χρωματισμών και λεπτομέρειες για το πως διαβάζονται τα πλέγματα αυτά παρουσιάζονται στην υπό-ενότητα **5.6.2 Απεικόνιση και Εξαγωγή Δεδομένων**.



Εικόνα 46 Στιγμιότυπο μετά την επιλογή του κουμπιού Start

Κατόπιν όπως είναι αναμενόμενο η επιλογή “Stop”, σταματάει την προσομοίωση. Για την επιτυχημένη παύση ο χρήστης μπορεί να ενημερωθεί και πάλι από το πλαίσιο κειμένου πάνω δεξιά (**Εικόνα 47**).



Εικόνα 47 Στιγμιότυπο μετά την επιλογή του κουμπιού Stop

Στο σημείο αυτό αξίζει να παρατηρηθεί πως μετά την εκκίνηση ή την παύση τα αντίστοιχα κουμπιά έχουν απενεργοποιηθεί και δεν είναι δυνατόν η επικοινωνία να

συνεχιστεί ούτε να επανεκκινηθεί. Σημειώνεται βέβαια, πως από την χρήση, αυτό δεν κατέστη πρόβλημα διότι δεν υπήρξαν περιπτώσεις που απαιτήθηκε παύση ούτε επανεκκίνηση, παρά μόνο στην διάρκεια ανάπτυξη της εφαρμογής.

Τέλος στην **Εικόνα 48**, παρουσιάζεται το παράθυρο μετά την “Export”, όπου το μόνο που διαφέρει είναι και πάλι η ενημέρωση στο πλαίσιο κειμένου πως η διαδικασία ολοκληρώθηκε και η εφαρμογή μπορεί να τερματιστεί.

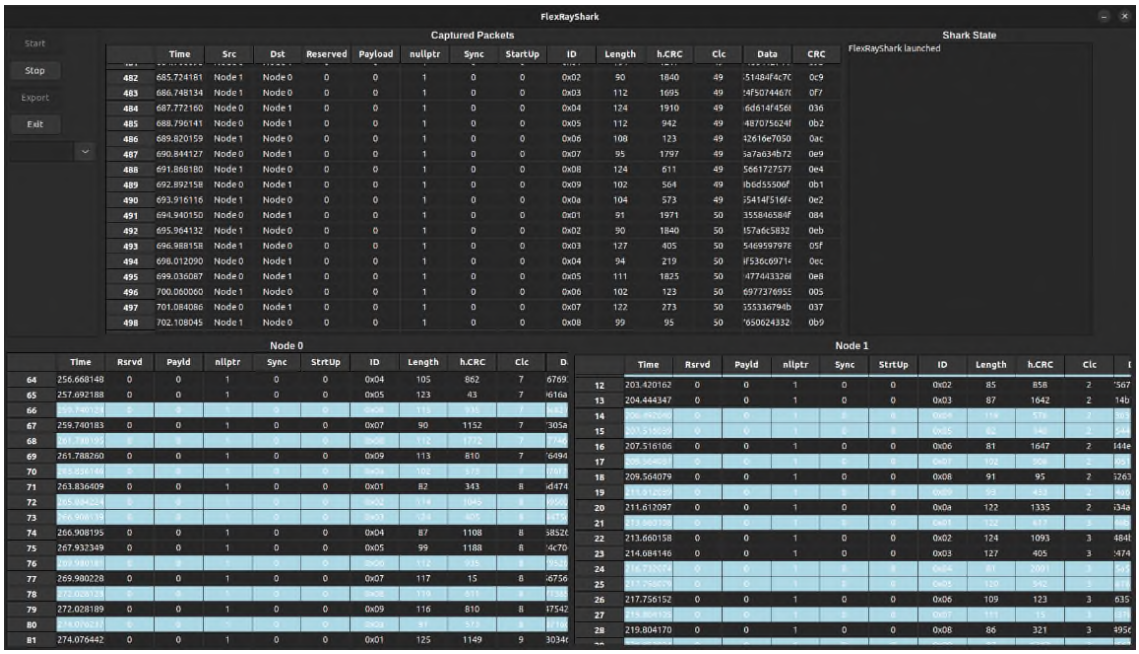
Εικόνα 48 Στιγμιότυπο μετά την επιλογή του κουμπιού Export

5.6.2 Απεικόνιση και Εξαγωγή Δεδομένων

Το παράθυρο του FlexRayShark, φιλοξενεί τρία πλέγματα δεδομένων με τρείς διαφορετικές ετικέτες το καθένα “Captured Packet ”, “Node 0” και “Node 1”. Σε αυτά εκτυπώνεται πληροφορία που προέρχεται από τα νήματα του λογισμικού FlexRayGen. Τα νήματα, όπως αναφέρθηκε στην προηγούμενη ενότητα, επικοινωνούν με το FlexRayShark μέσω ενός pipe. Το νήμα “Updator” λοιπόν της εφαρμογής διαβάζει το pipe, ακολουθώντας το πρωτόκολλο αποθήκευσης και ανάγνωσης δεδομένων που έχει οριστεί και ενημερώνει βάσει των πληροφοριών αυτών το αντίστοιχο πλέγμα.

5.6.2.1 Απεικόνιση Πλαισίων Σύλληψης

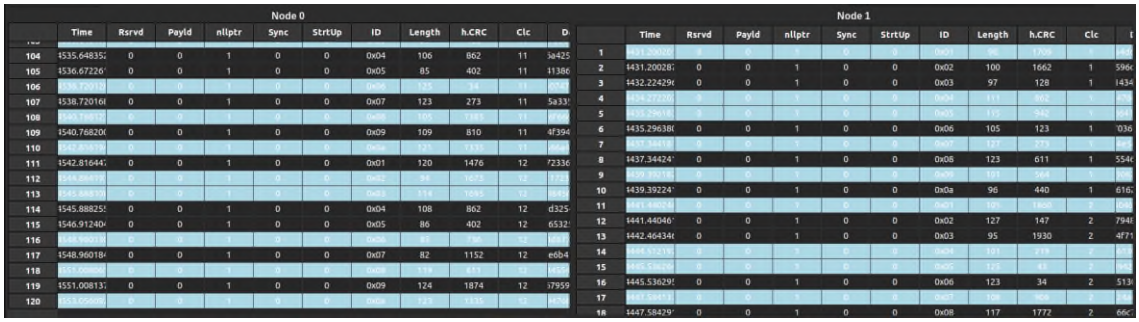
Το πρώτο πλέγμα περιέχει πληροφορίες για τον χρόνο, την πηγή και τον προορισμό, ακολουθούμενα από τα πεδία του FlexRay πλαισίου (**Εικόνα 49**). Τα πλαίσια τα οποία συμπληρώνουν το πλέγμα είναι πλαίσια που έχει συλλάβει το νήμα “Raptor” και σε αυτά περιλαμβάνονται τόσο τα αυθεντικά όσο και τα κακόβουλα σε περίπτωση επίθεσης. Κατά συνέπεια το πρώτο πλέγμα αποτελεί μια αναλυτική απεικόνιση της κίνησης τους δικτύου ανάμεσα στους κόμβους. Προβάλλεται η πηγή και ο προορισμός βάσει του αναγνωριστικού που έχει ανατεθεί σε καθένα, αλλά και ο ακριβής χρόνος που έγινε η σύλληψη του πλαισίου, σε μορφή χιλιοστών του δευτερολέπτου. Τέλος τις πληροφορίες αυτές ακολουθούν δεδομένα σχετικά με το κάθε πλαίσιο.



Εικόνα 49 Στιγμιότυπο της απεικόνισης των συλληφθέντων πλαισίων

5.6.2.2 Απεικόνιση Πλαισίων Κόμβων

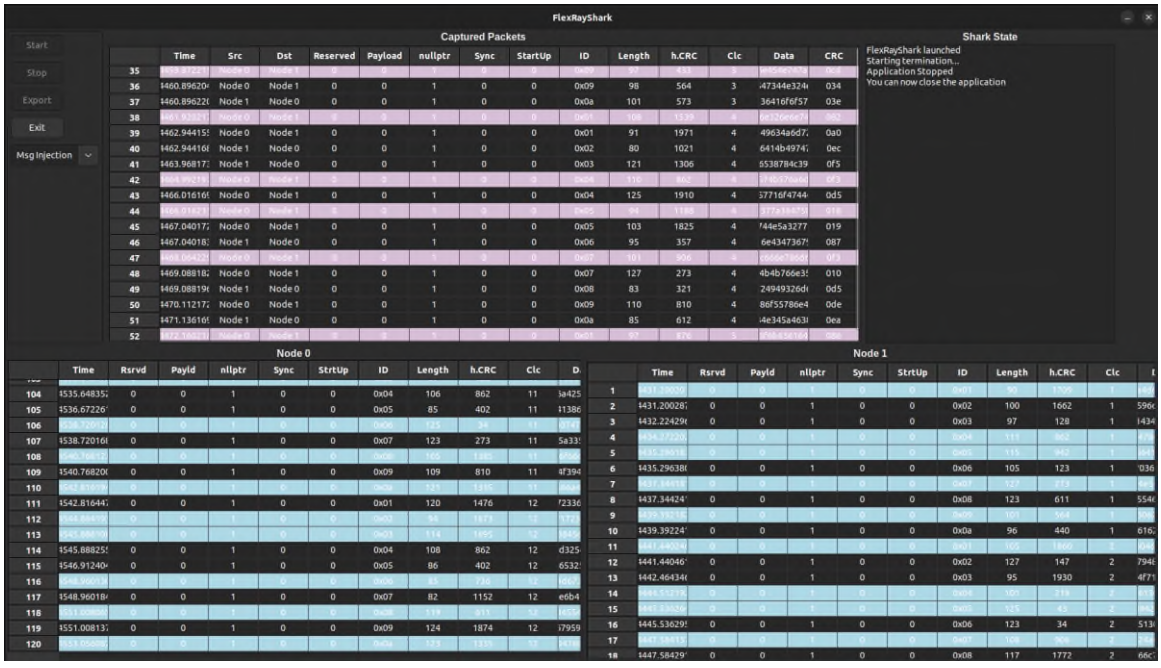
Με την ανάγνωση των κάτω πλαισίων ο χρήστης μπορεί να λάβει πλήρη εικόνα σε πραγματικό χρόνο των πλαισίων των οποίων κάθε κόμβος αποστέλλει ή λαμβάνει, καθώς και την στιγμή που αυτή λαμβάνει χρόνο (**Εικόνα 50**). Στο αριστερό πλέγμα υπάρχουν τα πλαίσια με τα οποία αλληλεπιδρά ο κόμβος 0 ενώ στο δεξί αυτά με τα οποία αλληλεπιδρά ο κόμβος 1. Το απαλό γαλάζιο χρώμα σημειώνει τα πλαίσια τα οποία λαμβάνει ο κόμβος, ενώ τα άχρωμα είναι αυτά που αποστέλλει.



Εικόνα 50 Στιγμιότυπο της απεικόνισης των πλαισίων μετάδοσης/λήψης του κάθε κόμβου

5.6.2.3 Απεικόνιση Επιθέσεων

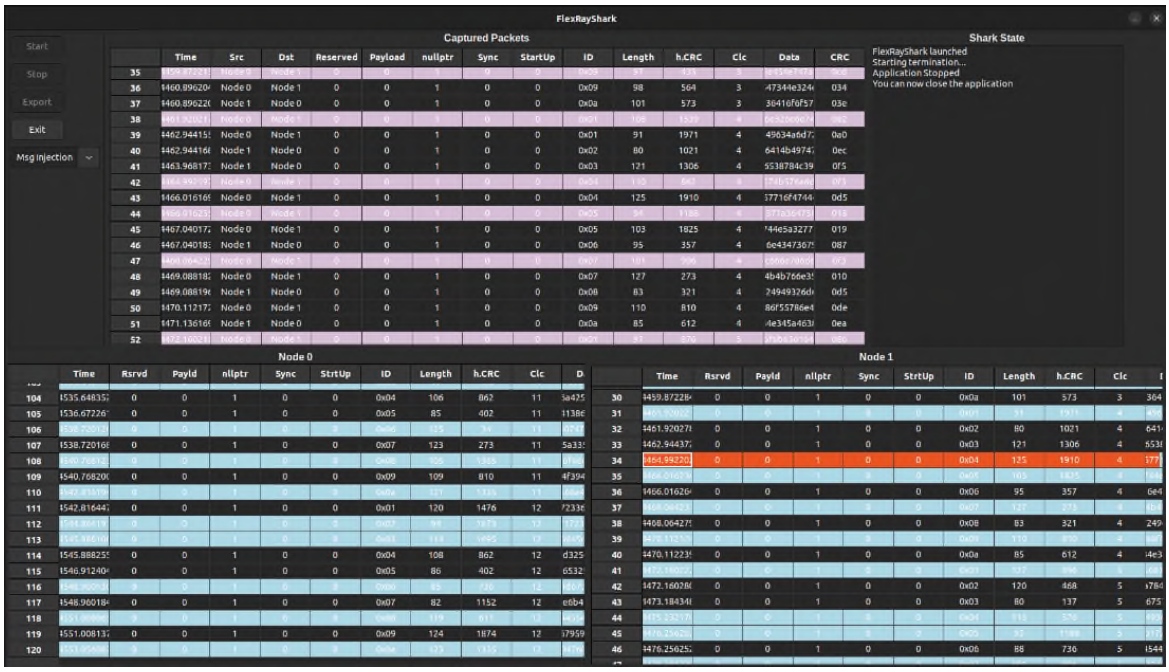
Για την σήμανση των επιθέσεων χρησιμοποιείται χρωματική κωδικοποίηση. Τα πλαίσια με χρώμα ροζ (**Εικόνα 51**), αφορούν πλαίσια που έχουν δεχτεί επίθεση επανάληψης πλαισίου.



Εικόνα 51 Στιγμιότυπο απεικόνισης πλαισίων κατά την εφαρμογή επίθεσης επανάληψης πλαισίου

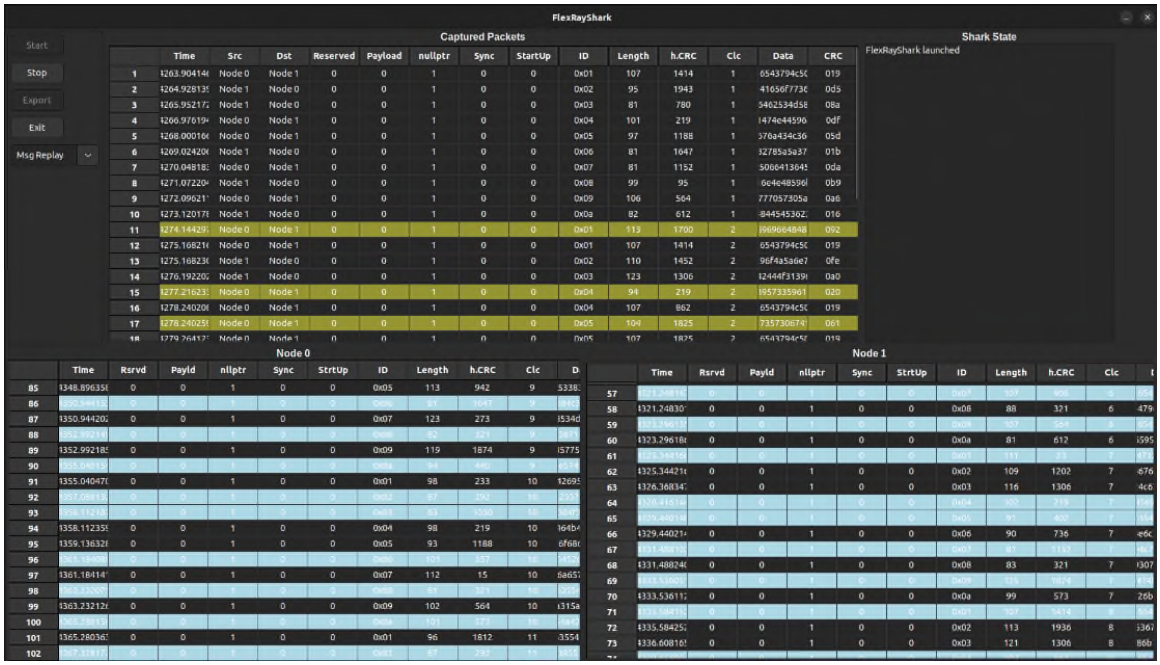
Υπογραμμίζεται πως τα χρωματισμένα πλαίσια είναι τα πλαίσια στόχος. Κατά συνέπεια τα κακόβουλα πλαίσια έπονται αμέσως μετά αυτών. Για παράδειγμα, όπως φαίνεται στην ακόλουθη εικόνα (**Εικόνα 52**), στο κύκλο 4 και στην χρονοθυρίδα 4, το πλαίσιο που έχει δεχτεί ο κόμβος 1 είναι αυτό που βρίσκεται ακριβώς κάτω από το

αντίστοιχο χρωματισμένο ροζ πλαίσιο που απεικονίζεται στο άνω κεντρικό πλέγμα. Οπότε ο χρωματισμός αφορά στο στοχευμένο πλαίσιο και το πλαίσιο που ακολουθεί αυτόν στο κακόβουλο.



Εικόνα 52 Στιγμιότυπο επαλήθευσης της εφαρμογής της επίθεσης

Αντίστοιχα τα πλαίσια με χρώμα κιτρινοπράσινο (**Εικόνα 53**) αφορούν πλαίσια που έχουν δεχτεί επίθεση έγχυσης πλαισίου. Και πάλι το κακόβουλο πλαίσιο έπεται του χρωματισμένου.



Εικόνα 53 Στιγμιότυπο απεικόνισης πλαισίων κατά την εφαρμογή επίθεσης έγχυσης πλαισίου

5.6.2.4 Εξαγωγή Δεδομένων

Η εξαγωγή των δεδομένων γίνεται με την επιλογή του αντίστοιχου κουμπιού από το πάνελ επιλογών. Οι πληροφορίες που εξάγονται αποθηκεύονται σε ένα αρχείο .csv, το όνομα του οποίου εξαρτάται από τις επιλογές του χρήστη. Στην περίπτωση που επιλέξει επίθεση επανάληψης πλαισίου στο κύριο κατάλογο, δηλαδή εκεί που αποθηκεύεται και το αρχείο καταγραφής, θα δημιουργηθεί ένα αρχείο με όνομα “replay.csv”. Στην περίπτωση της επίθεσης έγχυσης θα δημιουργηθεί ένα αρχείο με όνομα “injection.csv”, ενώ αν δεν επιλεγεί τύπος επίθεσης το αρχείο θα έχει όνομα “legit.csv”. Τα δεδομένα που εξάγονται είναι αυτά του πλέγματος του κόμβου Node 1 με την προσθήκη μιας επιπλέον κατηγορίας με όνομα “Malicious”, που προσδιορίζει αν το πλαίσιο αυτό είναι κακόβολου ή όχι. Για την σήμανση αυτή γίνεται παράλληλη ανάτρεξη και σύγκριση με τα πλαίσια του πλέγματος σύλληψης.

5.7 Μοντέλα Ανίχνευσης Ανωμαλιών

5.7.1 Support Vector Classification

Support Vector Machine ή εν συντομία SVM, είναι ένα σύνολο μεθόδων από εποπτευόμενους αλγορίθμους μάθησης (supervised learning algorithms) που χρησιμοποιούνται για προβλήματα classification και regressions. Για ορισμένα

δεδομένα στο επίπεδο, ψάχνει ένα υπέρ-επίπεδο (hyperplane) που να διαχωρίζει τα δεδομένα με τον καλύτερο τρόπο. Τα προβλήματα μπορούν να χωριστούν σε δύο κατηγορίες, σε αυτά που τα δεδομένα είναι γραμμικά διαχωρίσιμα (linear separable) και αυτά που είναι μη γραμμικά διαχωρίσιμα (non-linear separable). Όπως αναφέρει και το όνομα, τα γραμμικά είναι αυτά που μπορούν να διαχωριστούν με γραμμή ενώ τα μη γραμμικά αυτά που είναι αδύνατον να χωριστούν με γραμμή, οπότε τότε χρειάζεται να προσθέσουμε μια επιπλέον διάσταση για να προβάλλουμε τα δεδομένα σε αυτήν και εν συνεχεία να τα χωρίσουμε. Πέρα από το υπέρ-επίπεδο επίσης ψάχνουμε και ένα διάστημα απόφασης (decision boundary), δηλαδή ένα διάστημα γύρο από το υπέρ-επίπεδο στο οποίο ο διαχωρισμός είναι ασαφής. Οι μέθοδοι υπολογισμού αυτών των boundaries ονομάζονται Support Vector Classifiers (SVC).

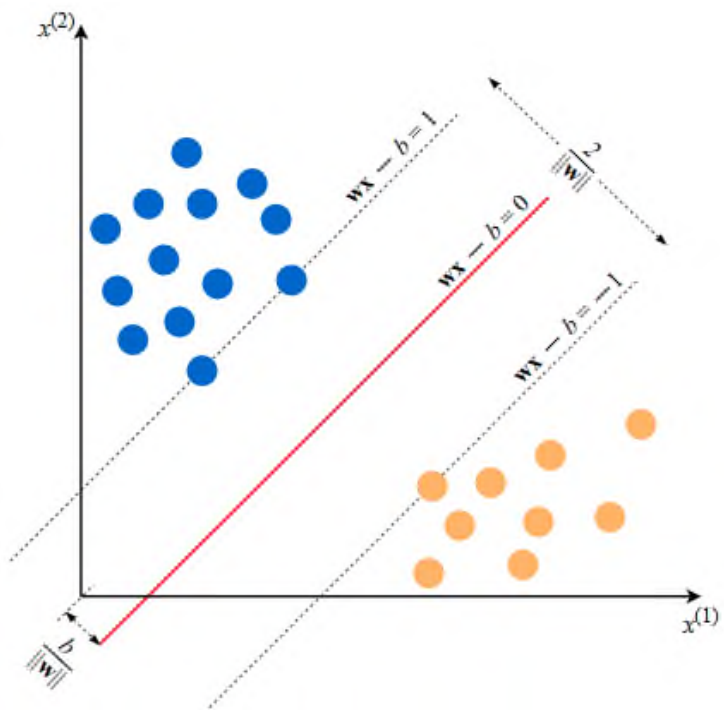
Λαμβάνοντας υπόψιν έναν separator και ένα σημείο, δηλαδή ένα δεδομένο, η απόσταση μεταξύ τους ονομάζεται margin και είναι θετική όταν το σημείο έχει ταξινομηθεί σωστά και αρνητική όταν έχει ταξινομηθεί στην λάθος κλάση. Μαθηματικά μπορεί να διαπιστωθεί από το γινόμενο του label του σημείου που βρίσκεται στο διάνυσμα y και της προσημασμένης απόστασης:

$$margin = y \times \text{signed\_}distance$$

Πιο συγκεκριμένα (**Εικόνα 54**) δεδομένου ενός πλήθους σημείων εκπαίδευσης $(x_1, y_1), \dots, (x_n, y_n)$ όπου το y_i μπορεί να πάρει τιμές 1 ή -1 και είναι μέρος του διανύσματος y που περιέχει τα labels των δειγμάτων, αναζητείται το υπέρ-επίπεδο με το μέγιστο περιθώριο (margin) ώστε να διαχωρίζει τα σημεία στις δύο κλάσεις σωστά. Κάθε υπέρ-επίπεδο μπορεί να εκφραστεί ως:

$$w^T x - b = 0$$

όπου w είναι ένα κανονικοποιημένο διάνυσμα.



Εικόνα 54 Support Vector Classification [73]

Στην περίπτωση των γραμμικά διαχωρίσιμων δεδομένων μπορεί να επιλεγεί το λεγόμενο “Hard Margin” ή το “Soft Margin”. Η διαφορά τους έγκειται στο πόσο αυστηρά ορίζουν το περιθώριο και διαχωρίζουν τα δεδομένα. Το πρώτο είναι απόλυτο και χρησιμοποιείται όταν δεν υπάρχει ανάγκη για ανεκτικότητα σε ακραίες τιμές (outliers) ενώ το δεύτερο επιτρέπει μικρά σφάλματα στην ταξινόμηση και είναι εφαρμόσιμο σε δεδομένα με ανακριβή παρατηρήσεις ή με ύπαρξη θορύβου.

Στην περίπτωση των μη γραμμικά διαχωρίσιμων δεδομένων για να εκπαιδευτεί ένας ταξινομητής, πρέπει να γίνουν πράξεις με διανύσματα υψηλών διαστάσεων στον μετασχηματισμένο χώρο των χαρακτηριστικών, γεγονός που οδηγεί σε εξαιρετικά υψηλό και μη πρακτικό υπολογιστικό κόστος. Για την επίλυση του προβλήματος αυτού χρησιμοποιούνται τα λεγόμενα “kernel tricks” τα οποία αντί να εφαρμόζουν τους μετασχηματισμούς και εν συνεχεία την προβολή των δεδομένων σε μεγαλύτερη διάσταση, αντιπροσωπεύουν τα σημεία μόνο μέσω ενός συνόλου ανά ζεύγη συγκρίσεων ομοιότητας μεταξύ των αρχικών παρατηρήσεων x. Η ομοιότητα εκφράζεται μέσω του εσωτερικού γινομένου δύο διανυσμάτων. Οι διαθέσιμοι kernels για αυτή την τεχνική είναι πολλοί, με δύο από τους διασημότερους τους:

Sigmoid Kernel $$K(x\_1, x\_2) = tanh(ax\_1\text{^}Tx\_2 + c)$$

Radial Basis Function Kernel (RBF) $K(x_1, x_2) = exp\left(-\gamma\left||x_1 - x_2|\right|^2\right),\ \gamma > 0$

Η SVC ξεχωρίζει διότι:

- είναι αποτελεσματική σε μεγάλες διαστάσεις και κυρίως όταν είναι μεγαλύτερες από το πλήθος των δεδομένων
- είναι αποδοτική ως προς την μνήμη αφού χρησιμοποιεί ένα σύνολο από σημεία εκπαίδευσης στην συνάρτηση απόφασης
- διαθέτει πολλές επιλογές ως προς τους πυρήνες (kernels) που μπορούν να χρησιμοποιηθούν ως συναρτήσεις αποφάσεων

αλλά

- εάν το πλήθος των χαρακτηριστικών (features) είναι μεγαλύτερο από αυτό των δειγμάτων απαιτεί κανονικοποίηση για την αποφυγή της υπέρ-προσαρμογής (over-fitting) και
- δεν προσφέρει εκτιμήσεις πιθανοτήτων αλλά χρησιμοποιεί μια ακριβή διαδικασία διασταυρωμένης επικαιροποίησης (cross-validation)

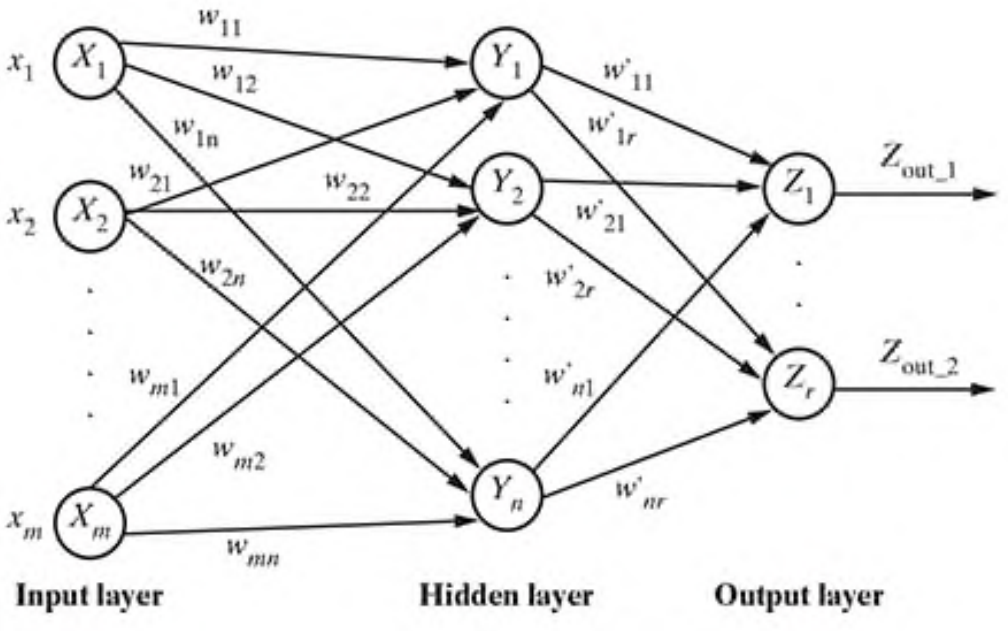
5.7.2 Feed Forward Neural Network (FFNN)

Ο αλγόριθμος μάθησης ενός νευρωνικού δικτύου μπορεί να είναι είτε supervised ή unsupervised. Ένα νευρωνικό δίκτυο λέγεται πως μαθαίνει supervised, αν η επιθυμητή έξοδος είναι γνωστή. Οι περιορισμοί τους είναι πως

- απαιτούν labeled δεδομένα,
- αποδίδουν καλύτερα όταν υπάρχουν πολλά δεδομένα
- απαιτούν ομοιογενή δεδομένα και
- πολλά προβλήματα δεν απαιτούν πρόβλεψη

Αποτελείται από ένα πλήθος κόμβων οι οποίοι χωρίζονται σε επίπεδα (**Εικόνα 55**). Αυτά είναι κυρίως τρία το input layer, το hidden layer και το output layer. Το hidden layer μπορεί να είναι ένα (Single-layer) ή πολλά (Multi-layer). Το input layer συνδέεται με το hidden και αυτό στην συνέχεια με το output. Στις ακμές που τα ενώνουν υπάρχουν τα βάρη (weights) και επίσης χαρακτηρίζονται και από μια συνάρτηση ενεργοποίησης (activation function) που παράγει το τελικό αποτέλεσμα που θα

περάσει στο επόμενο επίπεδο. Ο όρος εμπρόσθιας τροφοδοσίας (Feed Forward) έχει να κάνει με το γεγονός πως στην αρχιτεκτονική η πληροφορία ρέει από την είσοδο στην έξοδο χωρίς να υπάρχουν κλειστές διαδρομές ή ανατροφοδοτήσεις.



Εικόνα 55 Αρχιτεκτονική ενός FFNN [75]

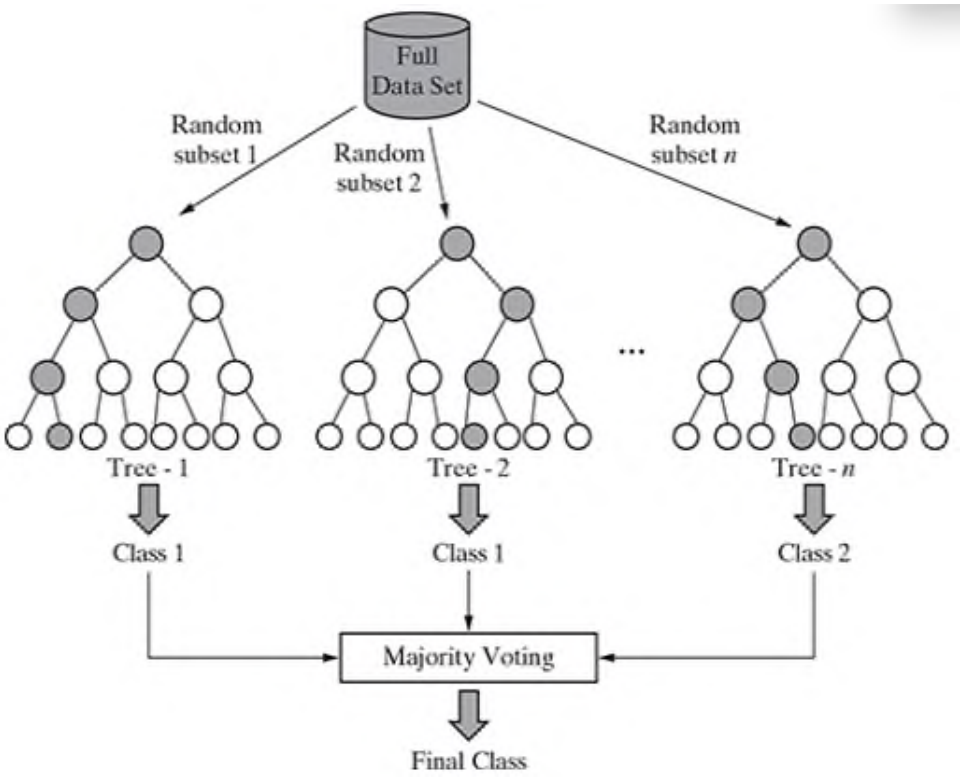
Οι επιλογές του μελετητή έχουν να κάνουν με το

- αν θα επιλεγεί και σε τι ποσοστό να εφαρμοστεί dropout, δηλαδή κατά την εκτέλεση του τρέχοντος time step αν ορισμένοι τυχαίοι κόμβοι δεν θα ληφθούν υπόψιν. Αυτό γίνεται για να μειωθεί το over-fitting.
- μέγεθος του batch, δηλαδή ο αριθμός των δειγμάτων εκπαίδευσης που χρησιμοποιούνται σε κάθε επανάληψη
- το πλήθος των hidden layers
- το πλήθος των κόμβων ανά επίπεδο
- τις συναρτήσεις ενεργοποίησης του κάθε επιπέδου
- την κανονικοποίηση ή μη των δεδομένων κάθε επιπέδου και
- το πλήθος των επαναλήψεων (epochs)

5.7.3 Random Forest

Το μοντέλο αυτό ανήκει στην κατηγορία των Ensemble Learning αλγορίθμων, δηλαδή συνδυάζει αποτελέσματα πολλών δέντρων αποφάσεων (**Εικόνα 56**) προκειμένου να

βελτιώσει την ακρίβεια του. Κάθε δέντρο εκπαιδεύεται σε ένα υποσύνολο δεδομένων και λαμβάνει αποφάσεις μόνο για τα χαρακτηριστικά που έχει τυχαία επιλέξει. Ο λόγος που χρησιμοποιείται μεγάλο πλήθος δέντρων είναι για να εκπαιδευτούν τα δέντρα αρκετά ώστε η συνεισφορά από ένα feature να εμφανίζεται σε πολλά μοντέλα. Μετά την δημιουργία του από τον συνδυασμό των δέντρων, οι έξοδοι καθενός συμψηφίζονται.



Εικόνα 56 Αρχιτεκτονική μοντέλου Random Forest [75]

Ο μελετητής κατά την εφαρμογή του μπορεί να ρυθμίσει το πλήθος των estimators δηλαδή των δέντρων. Αν το πλήθος των δέντρων είναι πολύ μεγάλο τότε το μοντέλο ίσως εμφανίσει υπέρ-προσαρμογή. Σε αυτήν την περίπτωση το μοντέλο θα μιμηθεί τα δεδομένα εκπαίδευσης και το σφάλμα εκπαίδευσης θα είναι σχεδόν μηδέν, όμως κατά τον έλεγχο σε διαφορετικά δεδομένα θα είναι υψηλό.

Στην γενική περίπτωση

- ανταποκρίνεται πολύ καλά σε μεγάλα σύνολα δειγμάτων,
- διαθέτει μια ισχυρή μέθοδο εκτίμησης των δεδομένων που λείπουν και διατηρεί την ακρίβεια του όταν το ποσοστό αυτών είναι μεγάλο.

- έχει ισχυρές μεθόδους εξισορρόπησης σφαλμάτων σε πληθυσμό κλάσεων μη ισορροπημένων σε σύνολα δεδομένων
- δίνει εκτιμήσεις σχετικά με το ποια features είναι πιο σημαντικά κατά την ταξινόμηση και
- τα παραγόμενα δέντρα μπορούν να αποθηκευτούν και χρησιμοποιηθούν και σε άλλα δεδομένα

5.7.4 k Nearest Neighbors

Πρόκειται για ένα πολύ ισχυρό αλγόριθμο ταξινόμησης, χωρίς παραμέτρους, στον οποίο τα άγνωστα και unlabeled δεδομένα που εισέρχονται για πρόβλεψη κρίνονται βάση της ομοιότητας με τα δεδομένα εκπαίδευσης και ταξινομούνται σε συστάδες (clusters). Ο μηχανικός του προσδιορίζει το πλήθος των k clusters και αυτό τα χωρίζει σε k συστάδες στηριζόμενος στις ιδιότητες των χαρακτηριστικών. Κάθε νέο δείγμα ταξινομείται στο cluster που είναι πιο στενά συνδεδεμένα μεταξύ του από άποψη ομοιότητας. Η μέτρηση της ομοιότητας δύο δεδομένων στηρίζεται στην ευκλείδεια απόσταση:

$$\text{Euclidean distance} = \sqrt{(f_{11} - f_{12})^2 + (f_{21} - f_{22})^2}$$

όπου ο πρώτος δείκτης συμβολίζει το δείγμα και ο δεύτερος το features.

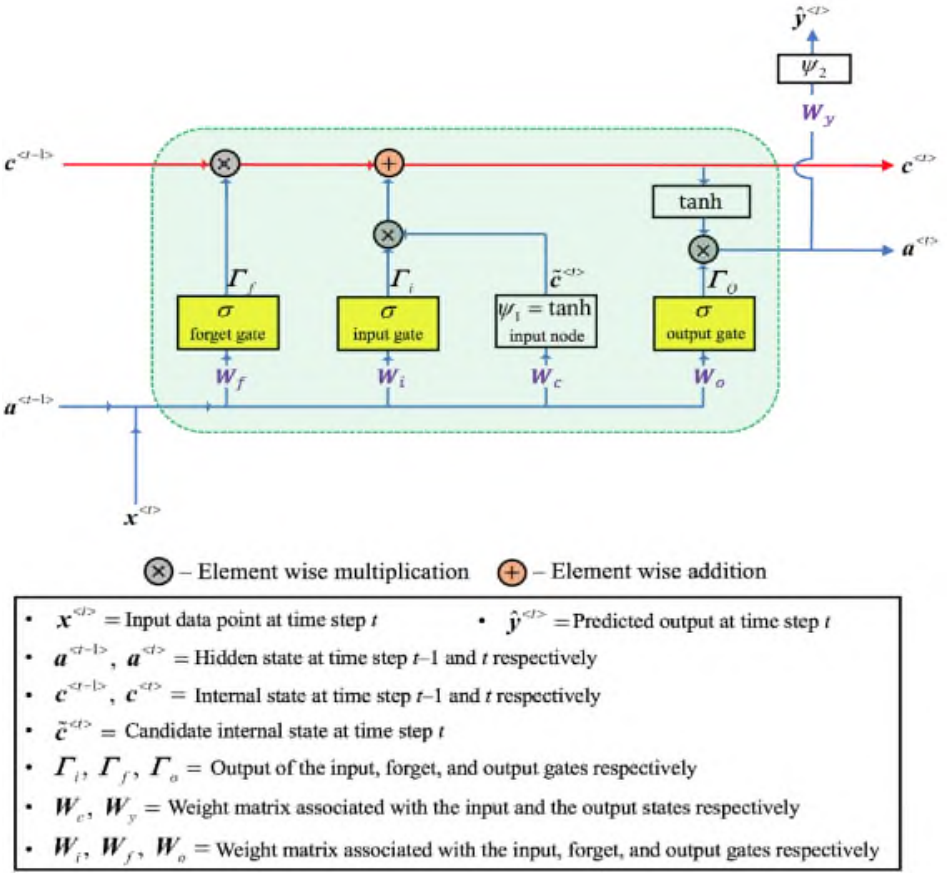
Το μοντέλο αυτό ξεχωρίζει διότι:

- είναι πολύ απλό, εύκολο στην κατανόηση και αποδοτικό σε αρκετές περιπτώσεις
- είναι γρήγορο στην εκπαίδευση του αλλά
- δεν μαθαίνει τίποτα στην πράξη. Η ταξινόμηση γίνεται βάση των δεδομένων εκπαίδευσης, με αποτέλεσμα να έχει μεγάλη συσχέτιση με αυτά

5.7.5 Long Short-Term Memory (LSTM)

Μερικές φορές για να ολοκληρωθεί ένας στόχο, όπως μια πρόβλεψη, χρειάζεται το πρόσφατο παρελθόν ενώ σε άλλες το πιο μακρινό παρελθόν. Το LSTM είναι μια ειδική κατηγορία αναδρομικού νευρωνικού δικτύου (RNN) ικανό να μαθαίνει long-term εξαρτήσεις, αφού θυμάται πληροφορία για μεγάλες χρονικές περιόδους. Ως RNN έχει μια δομή σε μορφή αλυσίδας (**Εικόνα 57**), όπου το σημείο κλειδί του LSTM είναι η

κατάσταση του cell, που μοιάζει με ιμάντα ο οποίος διατρέχει απευθείας ολόκληρη την αλυσίδα, με μερικές μόνο μικρές γραμμικές αλληλεπιδράσεις. Μέσω αυτού πληροφορίες ρέουν κατά μήκος της αλυσίδας πολύ εύκολα παραμένοντας αμετάβλητες. Το LSTM έχει τη δυνατότητα να αφαιρεί ή να προσθέτει πληροφορίες στο cell state, ρυθμιζόμενη προσεκτικά από δομές που ονομάζονται gates.



Εικόνα 57 Αρχιτεκτονική ενός LSTM μοντέλου [74]

Τα gates αποτελούνται από ένα επίπεδο με sigmoid ή tanh συνάρτηση ενεργοποίησης και μια λειτουργία πολλαπλασιασμού. Το επίπεδο αυτό εξάγει αριθμούς μεταξύ 0 και 1, περιγράφοντας πόση πληροφορία θα πρέπει να περάσει στο memory cell. Σε ένα μοντέλο LSTM υπάρχουν το input gate που καθορίζει πόση πληροφορία θα περάσει μέσα στο memory cell, το forget gate που είναι υπεύθυνο για τον καθορισμό της πληροφορίας που πρέπει να πεταχτεί από ένα memory cell και το output gate που καθορίζει πόση πληροφορία θα περάσει στο επόμενο time step.

Η LSTM ξεχωρίζει από τα RNN μοντέλα διότι:

- αποδίδει πολύ καλά σε μακροπρόθεσμες εξαρτήσεις ακολουθιακών δεδομένων αφού είναι ικανό να '*θυμάται*' ή να '*ξεχνά*' πληροφορίες. Κατά συνέπεια είναι κατάλληλη για επεξεργασία κειμένων, μεταφράσεων, αναγνώριση φωνής κτλ.
- είναι ανθεκτική και αποδοτική σε δεδομένα με ελλιπές ή θορυβώδη τιμές στα features, λόγω της λειτουργίας της forget gate, όμως επίσης
- είναι ακριβή υπολογιστικά, ιδίως για μεγάλα σύνολα δεδομένων
- έχει την τάση για υπέρ-προσαρμογή σε μικρά σύνολα δεδομένων
- διαθέτει πολλές υπέρ-παραμέτρους που απαιτούν ρύθμιση
- και απαιτεί πολλά δείγματα δεδομένων σε περιπτώσεις περίπλοκων μοτίβων στα δεδομένα, για να αποδώσει ικανοποιητικά

6. Πειράματα και Αποτελέσματα

6.1 Παρουσίαση Δεδομένων

Τα δεδομένα τα οποία χρησιμοποιήθηκαν για εκπαίδευση και έλεγχο των υπό μελέτη μοντέλων είναι αποτέλεσμα της εκτέλεσης του FlexRayShark. Πιο συγκεκριμένα, επιλέχθηκαν να παραχθούν σύνολα δεδομένων με πολλά και λίγα δείγματα και σύνολα με υψηλή, χαμηλή και πολύ χαμηλή συχνότητα ή πιθανότητα εκδήλωσης επίθεσης. Τα σύνολα αυτά συνοψίζονται στον ακόλουθο πίνακα (**Πίνακας 1**).

Πίνακας 1 Σύνολα δεδομένων που χρησιμοποιήθηκαν στα πειράματα

Όνομα	Μέγεθος	$F_{επίθεσης}$ / $P_{επίθεσης}$
legit60.csv	60 κύκλοι επικοινωνίας	-
legit12.csv	12 κύκλοι επικοινωνίας	-
replay60H.csv	60 κύκλοι επικοινωνίας	Υψηλή
replay12H.csv	12 κύκλοι επικοινωνίας	Υψηλή
replay12L.csv	12 κύκλοι επικοινωνίας	Χαμηλή
replay12VL.csv	12 κύκλοι επικοινωνίας	Πολύ Χαμηλή
injection60H.csv	60 κύκλοι επικοινωνίας	Υψηλή
injection12H.csv	12 κύκλοι επικοινωνίας	Υψηλή
injection12L.csv	12 κύκλοι επικοινωνίας	Χαμηλή
injection12VL.csv	12 κύκλοι επικοινωνίας	Πολύ Χαμηλή

Η μορφή των δεδομένων εντός των συνόλων αυτών μοιάζει με αυτό που παρουσιάζεται στην ακόλουθη εικόνα (**Εικόνα 58**).

	Time	Src	Dst	reserved	payload	nullptr	sync	startup	data	CRC	Malicious	id	length	h.CRC	clc
39.036138	Node 0	Node 1	0	0	1	0	0	6173646b6c66616b6c6661343934693061347661703961...	073	0	0x01	96	1812	1
40.060129	Node 1	Node 0	0	0	1	0	0	6173646b6c66616b6c6661343934693061347661703961...	0ef	0	0x02	93	1292	1
41.084113	Node 1	Node 0	0	0	1	0	0	6861636575397533393861616375307061763461703075...	0a0	0	0x03	97	128	1
42.108111	Node 0	Node 1	0	0	1	0	0	6861636575397533393861616375307061763461703075...	08f	0	0x04	83	2001	1
43.132060	Node 0	Node 1	0	0	1	0	0	766e636e6b6e766e6a763868727334636e6e6834766237...	012	0	0x05	95	1188	1
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
48.316241	Node 1	Node 0	0	0	1	0	0	777961633869363834367169727796c69727673617677268...	05d	0	0x06	87	736	60
50.364219	Node 0	Node 1	0	0	1	0	0	4138434c636b616872633943594c6339386e3879593859...	0df	1	0x07	98	1797	60
50.364236	Node 1	Node 0	0	0	1	0	0	4138434c636b616872633943594c6339386e3879593859...	03f	0	0x08	100	1385	60
52.412050	Node 0	Node 1	0	0	1	0	0	414a524f5643554a757639554e56494e52484149434c4c...	057	1	0x09	122	1874	60
52.412075	Node 1	Node 0	0	0	1	0	0	414a524f5643554a757639554e56494e52484149434c4c...	0f4	0	0x0a	85	612	60

Εικόνα 58 Στιγμιότυπο απεικόνισης της μορφής των δεδομένων ενός συνόλου δεδομένων

6.2 Προεπεξεργασία Δεδομένων

Στην μηχανική μάθηση κατά το σχεδιασμό μοντέλων, ένα από τα κυριότερα στάδια και κρισιμότερα για την αποτελεσματικότητα αυτού είναι η μηχανική των χαρακτηριστικών (features engineering). Η εισαγωγή των δεδομένων αμιγώς χωρίς κάποια προεπεξεργασία, οδηγεί σε αποτελέσματα στα οποία η αποτελεσματική αναγνώριση των κακόβουλων πλαισίων είναι αρκετά αποθαρρυντική. Στον **Πίνακας 2**, παρουσιάζονται ενδεικτικά ορισμένα από αυτά.

Πίνακας 2 Επιλεγμένα αποτελέσματα από την εφαρμογή των δεδομένων στα μοντέλα χωρίς προεπεξεργασία

Model	Test set	Accuracy	Precision
linear SVC	20% of replay60H	50%	100%
			75%
	legit12	50%	100%
			0%
	replay12H	83%	100%
			67%
	replay12L	75%	100%
			50%
	repaly12VL	54%	100%
			8%
kNN	20% of replay60H	87%	95%
			77%
	legit12	53%	64%
			41%
	replay12H	53%	63%
			40%
	replay12L	62%	62%
			0
	replay12VL	96%	62%
			0%

Στα πλαίσια της προεπεξεργασίας των δεδομένων που εφαρμόστηκε, λοιπόν, τα βήματα είναι πολύ συγκεκριμένα. Όπως παρουσιάζεται και στην **Εικόνα 59**, αρχικά φορτώνεται το επιλεγμένο σύνολο δεδομένων ως DataFrame με την χρήση της βιβλιοθήκης *pandas*.

```
def split_string_into_substrings(string, substring_length):
        return [string[i:i+substring_length] for i in range(0, len(string), substring_length)]

def dataset_import(name, splitSize = 0):
    # Load
    df = pd.read_csv(name)
    # Map Values
    df['Src'] = df['Src'].map({'Node 0': 0, 'Node 1': 1})
    df['Dst'] = df['Dst'].map({'Node 0': 0, 'Node 1': 1})
    # Milliseconds difference from the first timestamp
    start_time   = df['Time'].iloc[0]
    df['msec'] = (df['Time'] - start_time)
    # Calculate delay
    df['delay'] = df['msec'].diff().fillna(0)
    # Convert hexadecimal values to integers
    df['id']   = df['id'].apply(lambda x: int(x, 16))
    df['CRC']   = df['CRC'].apply(lambda x: int(x, 16))
    df['data'] = df['data'].apply(lambda x: bytes.fromhex(x).decode('utf-8'))
    # Split to Substrings
    if splitSize:
        substring_length = splitSize
        subcolumns = df['data'].apply(lambda x: split_string_into_substrings(x, substring_length))
        num_columns = len(subcolumns.iloc[0])
        subcolumns_df = pd.DataFrame(subcolumns.tolist(), columns=[f'data_{i+1}' for i in range(num_columns)])
        label_encoder = LabelEncoder()
        for col in subcolumns_df.columns:
            subcolumns_df[col] = label_encoder.fit_transform(subcolumns_df[col])
        df = pd.concat([df, subcolumns_df], axis=1)
        df = df.drop(columns=['data'])
    else:
        label_encoder = LabelEncoder()
        df['data'] = label_encoder.fit_transform(df['data'])
    # Drop Data
    df = df.drop('Time', axis='columns')
    df = df.drop(columns=['reserved'])
    df = df.drop(columns=['payload'])
    df = df.drop(columns=['nullptr'])
    df = df.drop(columns=['sync'])
    df = df.drop(columns=['startup'])
    return df
```

Εικόνα 59 Στιγμιότυπο αλγορίθμου προεπεξεργασίας των δεδομένων

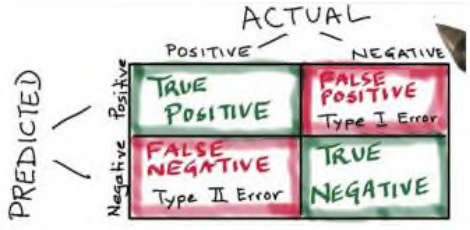
Αμέσως μετά οι κατηγορικές τιμές του προορισμού και της πηγής, αντιστοιχίζονται στα ψηφία 0 και 1 και λίγο έπειτα οι δεκαεξαδικές τιμές των πεδίων *id*, *CRC* και *data* μετατρέπονται σε ακεραίους. Η στήλη που αντιστοιχεί στον χρόνο, υπολογίζεται για όλο το σύνολο ως η διαφορά από την πρώτη τιμή, ενώ επίσης προστίθεται και μια επιπλέον στήλη που υπολογίζεται ως η διαφορά μεταξύ διαδοχικών χρονικών στιγμών και κατά συνέπεια εκφράζει την καθυστέρηση (*delay*). Λόγω της φύσης της προσομοίωσης όπως παρουσιάστηκε σε προηγούμενες ενότητες τα πεδία *reserved*, *payload* , *nullptr*, *sync* και *startup* μεταξύ όλων των πλαισίων περιέχουν την ίδια τιμή και έτσι παραλείπονται από το τελικό σύνολο. Τέλος ιδιαίτερο χειρισμό λαμβάνει το κομμάτι των δεδομένων. Σε μια πραγματική εφαρμογή μιας FlexRay επικοινωνίας η

μονάδα ηλεκτρονικού ελέγχου ακολουθεί για το κομμάτι των δεδομένων μια πολιτική από κανόνες προκειμένου να πραγματοποιείται η επικοινωνία. Επίσης το τμήμα αυτό φέρει πληροφορίες για συγκεκριμένα τμήματα και αισθητήρες του τομέα στον οποίο ανήκει. Αυτό έχει ως αποτέλεσμα τα πεδία αυτά, μεταξύ διαφορετικών πλαισίων του ίδιου όμως σκοπού – όπου με το σκοπό αναφερόμαστε στο αν το πλαίσιο είναι κενό, πλαίσιο συγχρονισμού, στατικού τμήματος κτλ. – να εμφανίζουν ομοιότητα ή κάποιας μορφής μοτίβων. Έτσι λοιπόν κατά την φόρτωση ενός συνόλου δεδομένων δίνεται η δυνατότητα τεμαχισμού του τμήματος των δεδομένων σε συγκεκριμένο μέγεθος. Είτε επιλεγεί τεμαχισμός είτε όχι, για τα τμήματα ή για το τμήμα αντίστοιχα, γίνεται χρήση του *LabelEncoder* της *sklearn* βιβλιοθήκης, που εφαρμόζει κωδικοποίηση βάση ενός σχήματος τακτικής κωδικοποίησης.

6.3 Αξιολόγηση Αποτελεσμάτων

Πολύ σημαντική επίσης είναι η σωστή αξιολόγηση των αποτελεσμάτων. Υπάρχουν συγκεκριμένες μετρικές που χρησιμοποιούνται για τον σκοπό αυτό και διαφέρουν αναλόγως το μοντέλο, τα δεδομένα και το τύπο του προβλήματος. Το πρόβλημα στην εργασία αυτή είναι πρόβλημα ταξινόμησης και παρακάτω παρουσιάζονται οι μετρικές που επιλέχθηκαν στην παρούσα εργασία.

1. *Confusion Matrix*: πρόκειται για έναν πίνακα (**Εικόνα 60**) που περιγράφει την απόδοση ενός μοντέλου ταξινόμησης σε ένα σύνολο από δεδομένα δοκιμής για τα οποία είναι γνωστές οι αληθείς τιμές.



Εικόνα 60 Μορφή πίνακα του σύγχυσης

Ως αληθές θετικό ή αρνητικό χαρακτηρίζεται ένα δεδομένο του οποίου η ταξινόμηση από το μοντέλο συνάδει με την πραγματική αληθή τιμή. Σε αντίθετη περίπτωση ταξινομείται ως εσφαλμένος αρνητική ή εσφαλμένος θετική, όπως προκύπτει από το όνομα.

2. *Accuracy*: ορίζεται ως ο αριθμός των σωστών προβλέψεων του μοντέλου προς το σύνολο αυτών. Με άλλα λόγια είναι το άθροισμα των αληθώς θετικών και αρνητικών προς το άθροισμα όλων των αξιολογήσεων:

$$Accuracy = \frac{TP + FP}{TP + FP + FN + TN}$$

3. *Precision»*: αναφέρεται στο αριθμό των αληθώς θετικών προς το πλήθος των θετικών αληθών και εσφαλμένων.

$$Precision = \frac{TP}{TP + FP}$$

4. *Recall*: εκφράζει το πόσο συχνά ένα θετικό αποτέλεσμα προβλέπεται σωστά και ορίζεται ως

$$Recall = \frac{TP}{TP + FN}$$

5. *F1-score*: πρόκειται για το ζυγισμένο μέσο όρο των δύο προηγούμενων μετρικών

$$F_1 = 2 \times \frac{precision \times recall}{precision + recall}$$

Πρέπει να τονιστεί πως μια μετρική μόνο, δεν μπορεί να δώσει επαρκή και ασφαλή εικόνα για την επίδοση ενός μοντέλου. Για παράδειγμα κατά την δοκιμή ενός μοντέλου είναι πιθανό να εμφανιστεί υψηλό ποσοστό ακρίβειας, όμως μια πιο λεπτομερή μελέτη και συγκεκριμένα στην μετρική Precision μπορεί να δείξει πως καμία επίθεση δεν ανιχνεύτηκε. Έτσι κρίνεται εξαιρετικά σπουδαία η επισκόπηση όλων των αναφερθέντων μετρικών προκειμένου να διαπιστωθεί η εγκυρότητα ενός αποτελέσματος.

6.4 Μεθοδολογία Πειραμάτων

Η μέθοδος που ακολουθήθηκε για την εκτέλεση των πειραμάτων ήταν αρχικά η φόρτωση, με τον τρόπο που περιγράφηκε στην υπό-ενότητα **6.2 Προεπεξεργασία Δεδομένων**, του συνόλου δεδομένων των πολλών δειγμάτων και της υψηλής συχνότητας εμφάνισης της εκάστοτε επίθεσης και κατόπιν η εκπαίδευση του επιλεγμένου μοντέλου σε μέρος αυτού. Το σύνολο χωρίστηκε κατά 80% και 20% σε σύνολο εκπαίδευσης και δοκιμής αντίστοιχα. Επόμενο βήμα μετά την εκπαίδευση και

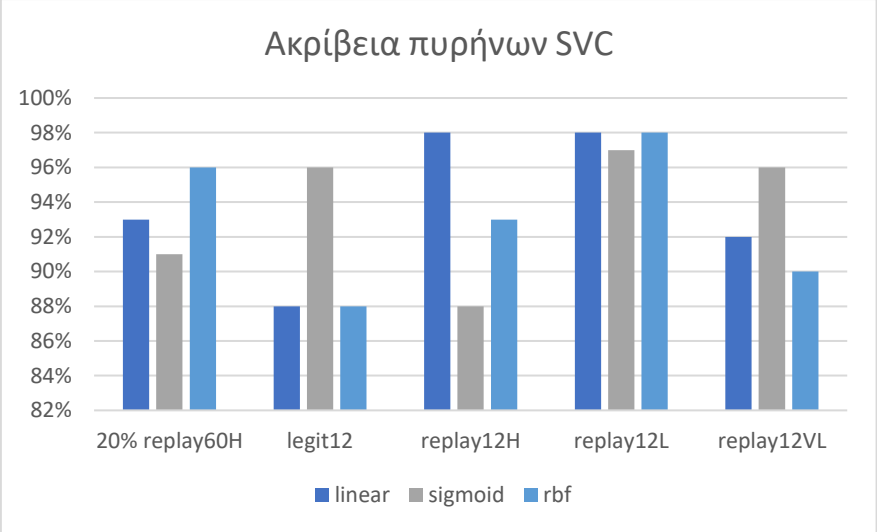
τον έλεγχο του μοντέλου είναι η στοχευμένη δοκιμή του. Για το στάδιο αυτό φορτώθηκαν με τον ίδιο τρόπο όλα τα σύνολα δεδομένων με λίγα δείγματα και ελέγχθηκαν για την αποδοτικότητα τους ένα προς ένα. Κατ' επέκταση κάθε μοντέλο δοκιμάζεται σε πλήρως αυθεντικά δεδομένα, σε δεδομένα υψηλής, χαμηλής και πολύ χαμηλής συχνότητας επιθέσεων. Επειδή, λοιπόν, κάθε σύνολο έχει διαφορετική συχνότητα εμφάνισης των επιθέσεων, ήταν πολλές οι φορές που το μοντέλο προκειμένου να αποδώσει εξειδικεύτηκε αποκλειστικά για το εκάστοτε σύνολο. Μέχρι την λήψη επιτρεπτών αποτελεσμάτων, οι παράμετροι κάθε μοντέλου ρυθμίστηκαν πολλές φορές και με διαφορετικούς τρόπους, ανάλογα φυσικά με την εκάστοτε επίδοση. Στα πλαίσια αυτών των παραμέτρων εντάσσεται και η κατάτμηση αλλά και η επιλογή συγκεκριμένων στηλών. Ένα σύνολο που περιέχει χαρακτηριστικά που εκφράζουν χρόνο και ένα μοντέλο προσανατολισμένο σε αυτά, εφαρμόζει μια χρονικά βασισμένη ανίχνευση. Αντιθέτως η αφαίρεση των στηλών αυτών και η διατήρηση των πεδίων των δεδομένων, αφορά μια ανίχνευση βασισμένη στα δεδομένα. Στην πλειοψηφία των μοντέλων επιλέχθηκε και απέδωσε, όπως θα φανεί παρακάτω, η υβριδική ανίχνευση, που περιλαμβάνει και τις δύο στήλες. Για την αξιολόγηση δόθηκε έμφαση στον συνδυασμό των μετρικών που αναφέρθηκαν προηγουμένως και έτσι στη σημασία του αποτελέσματος. Για παράδειγμα υπήρξαν μοντέλα με πολύ καλή συνολική ακρίβεια τα οποία όμως δεν εντόπιζαν κανένα από τα υπάρχοντα κακόβουλα πλαίσια.

6.5 Αποτελέσματα

6.5.1 Επίθεση Επανάληψης Πλαισίου

6.5.1.1 Support Vector Classification

Στην περίπτωση αυτή δοκιμάστηκαν τρείς πυρήνες και από τα αποτελέσματα παρατηρείται πως οι συναρτήσεις είναι ισοδύναμες και πως η επιλογή της κατάλληλης για την υψηλότερη επίδοση εξαρτάται από τα διαθέσιμα δεδομένα. Μια σύγκριση των τριών kenrels παρουσιάζεται στο **Διάγραμμα 1**.

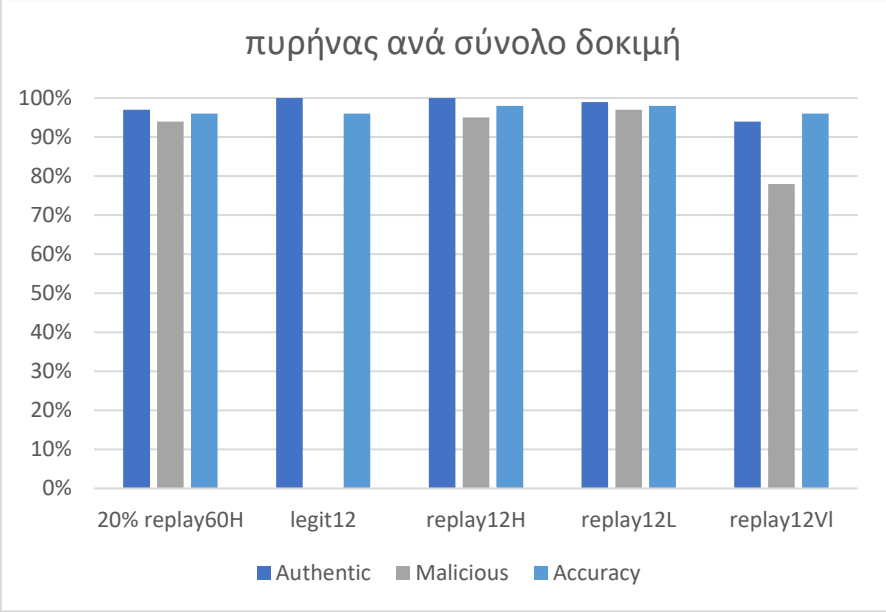


Διάγραμμα 1 Σύγκριση ακρίβειας πυρήνων μοντέλου SVC

Στον εντοπισμό των επιθέσεων στο σύνολο εκπαίδευσης, η καλύτερη ανίχνευση επιτυγχάνεται με τη συνάρτηση ακτινικής βάσης, ενώ στο σύνολο με την αυξημένη συχνότητα εμφάνισης η γραμμική. Στις χαμηλές συχνότητες ανταποκρίνονται πολύ καλά και οι τρείς με την ακτινική όμως να ξεχωρίζει ελαφρώς και στην πολύ χαμηλή συχνότητα δεν φαίνεται κάποιες από τις τρείς να είναι η κατάλληλη. Τέλος η ανίχνευση στο σύνολο μηδενικής συχνότητας, κατάλληλη είναι η σιγμοειδής με πολύ καλές μετρικές. Μια σύνοψη της καλύτερης ανά σύνολο δεδομένων επίδοσης παρουσιάζεται στον ακόλουθο **Πίνακας 3** και στο **Διάγραμμα 2**.

Πίνακας 3 Αποτελέσματα πειραμάτων ανίχνευσης επανάληψης πλαισίου με SVC

Kernel	Test set	Accuracy	Precision	Recall	F1-score
rbf	20% of	96%	97%	98%	97%
	replay60H		94%	91%	93%
sigmoid	legit12	96%	100%	96%	98%
			0%	0%	0%
linear	replay12H	98%	100%	98%	99%
			94%	100%	97%
rbf	replay12L	98%	99%	99%	99%
			97%	97%	97%
sigmoid	replay12VL	96%	97%	98%	98%
			78%	70%	74%



Διάγραμμα 2 Αποτελέσματα πειραμάτων ανίχνευσης επανάληψης πλαισίου με SVC

Σημειώνεται πως το πυρήνας rbf δεν φάνηκε να βοηθάει η κατάτμηση των δεδομένων και χρειάστηκε μέτρια προς υψηλή κανονικοποίηση και μικρή τιμή της παραμέτρου γ. Αντίστοιχα τους άλλους δύο πυρήνες εξυπηρέτησε η κατάτμηση σε μικρές ομάδες από Bytes και κανονικοποίηση όμοια της ακτινικής.

6.*5.1.2 Feed Forward Neural Network*

Το νευρωνικό δίκτυο που χρησιμοποιήθηκε στα πειράματα αποτελούντο από τρία επίπεδα με μεταβλητό πλήθος νευρώνων και είδος συνάρτησης ενεργοποίησης. Η επίδοση του ήταν ιδιαιτέρως απογοητευτική με ποσοστά επιτυχίας κάτω του 70%, με εξαίρεση τη δοκιμή του στο σύνολο εκπαίδευσης. Στην περίπτωση αυτή τα αποτελέσματα ήταν αρκετά καλά, όπως φαίνεται στον **Πίνακας 4**. Η εκπαίδευση του ήταν βασισμένη στον χρόνο και για το δίκτυο χρησιμοποιήθηκαν ως επίπεδο εισόδου 64 νευρώνες με συνάρτηση ενεργοποίησης Relu και κανονικοποίηση της τάξης των χιλιοστών της μονάδας. Το μεσαίο επίπεδο σχημάτισαν 32 νευρώνες με συνάρτηση ενεργοποίησης Leaky Relu και dropout 20%. Τέλος στο επίπεδο εξόδου εφαρμόστηκε η ίδια συνάρτηση με το επίπεδο εισόδου.

Πίνακας 4 Αποτελέσματα πειραμάτων ανίχνευσης επανάληψης πλαισίου με FFNN

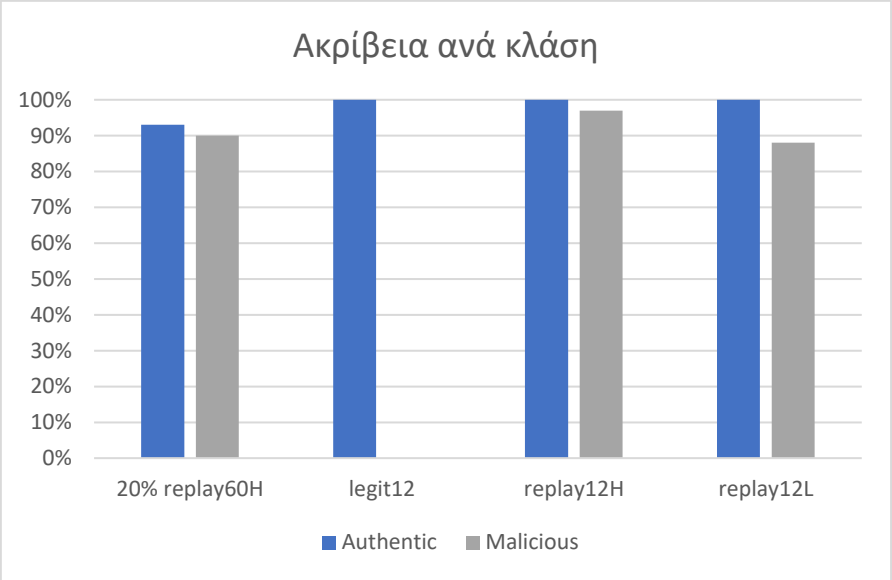
Test set	Accuracy	Precision	Recall	F1-score
20% of	96%	97%	98%	97%
replay60H		94%	91%	93%

6.5.1.3 Long Short-Term Memory

Τα πειράματα στο μοντέλο αυτό παρουσίασαν πολύ καλές επιδόσεις με εξαίρεση την περίπτωση ανίχνευσης επιθέσεων χαμηλής συχνότητας εμφάνισης. Οι μετρικές των τεσσάρων πειραμάτων που απέδωσαν παρουσιάζονται στο **Πίνακας 5** και στο **Διάγραμμα 3** γίνεται σύγκριση της ακρίβειας ανά κλάση πλαισίου. Γενικά χρησιμοποιήθηκε κατάτμηση μικρού έως και μηδενικού μεγέθους. Επίσης στις περιπτώσεις των υψηλών συχνοτήτων, καθοριστική ήταν η αφαίρεση των χαρακτηριστικών των χιλιοστών του δευτερολέπτου και της καθυστέρησης, και άρα η εφαρμογή ανίχνευσης βασισμένης στα δεδομένα.

Πίνακας 5 Αποτελέσματα πειραμάτων ανίχνευσης επανάληψης πλαισίου με LSTM

Test set	Accuracy	Precision	Recall	F1-Score
20% replay60H	93%	93%	97%	95%
		90%	82%	86%
legit12	100%	100%	100%	100%
		0%	0%	0%
replay12H	99%	100%	99%	99%
		97%	100%	99%
replay12L	97%	100%	96%	98%
		88%	100%	94%



Διάγραμμα 3 Αποτελέσματα πειραμάτων ανίχνευσης επανάληψης πλαισίου με LSTM

6.5.1.4 Random Forest

Το μοντέλο αυτό αποδείχτηκε εξαιρετικό για δύο μόνο περιπτώσεις (**Πίνακας 6**), αυτή της δοκιμής με το σύνολο εκπαίδευσης και αυτής με το σύνολο μηδενικής συχνότητας. Δεν απαίτησε κάποιο ποσοστό κατάτμησης των δεδομένων και λειτούργησε άψογα με ολόκληρο το πεδίο ακέραιο. Σημειώνεται βέβαια πως για την επιτυχία του απαιτήθηκαν 1000 επαναλήψεις (epochs) και στα δύο σενάρια. Σε κάθε

άλλη περίπτωση αδυνατούσε να ανιχνεύσει τις επιθέσεις ιδίως μάλιστα στην περίπτωση των χαμηλών συχνοτήτων απέτυχε παταγωδώς.

Πίνακας 6 Αποτελέσματα πειραμάτων ανίχνευσης επανάληψης πλαισίου με RF

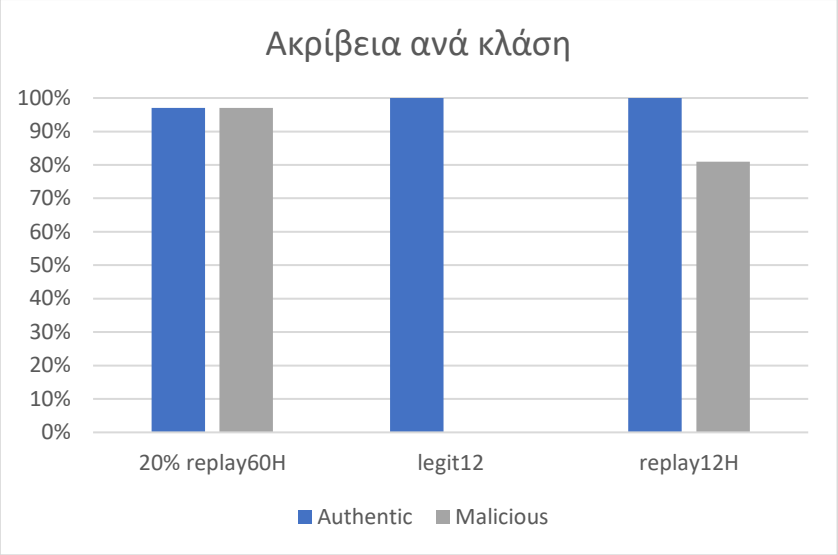
Test set	Accuracy	Precision	Recall	F1-score
20%	98%	100%	98%	99%
replay60H		94%	100%	97%
legit12	99%	100%	99%	100%
		0	0%	0%

6.5.1.5 k Nearest Neighbors

Οι μετρήσεις το ανέδειξαν μια εξαιρετική επιλογή κατά την δοκιμή με το σύνολο εκπαίδευσης και με το σύνολο των αποκλειστικά αυθεντικών πλαισίων. Στη δοκιμή του με το σύνολο υψηλής συχνότητας ανταποκρίθηκε επίσης αρκετά καλά, όχι όμως και στις άλλες δύο των χαμηλών συχνοτήτων. Τα αποτελέσματα από τα πειράματα στα τρία πρώτα σύνολα παρουσιάζονται στο **Πίνακας 7** και μια σύγκριση τους στο **Διάγραμμα 4**.

Πίνακας 7 Αποτελέσματα πειραμάτων ανίχνευσης επανάληψης πλαισίου με kNN

Test set	Accuracy	Precision	Recall	F1-score
20%	97%	97%	99%	98%
replay60H		97%	91%	94%
legit12	95%	100%	95%	97%
		0%	0%	0%
replay12H	93%	100%	91%	95%
		81%	100%	90%



Διάγραμμα 4 Αποτελέσματα πειραμάτων ανίχνευσης επανάληψης πλαισίου με kNN

Επίσης το παρόν μοντέλο παρουσιάζεται αρκετά ευαίσθητο στην επιλογή μικρού μεγέθους κατάτμησής των δεδομένων, και ιδίως μικρού πλήθους της γειτόνων κατά την διαδικασία πρόβλεψης. Στις δύο πρώτες περιπτώσεις πολύ σημαντική κρίθηκε, ταυτόχρονα και η αφαίρεση της στήλης των χιλιοστών του δευτερολέπτου, όχι όμως της στήλης της καθυστέρησης.

6.5.2 Επίθεση Έγχυσης Πλαισίου

6.5.2.1 Support Vector Classification

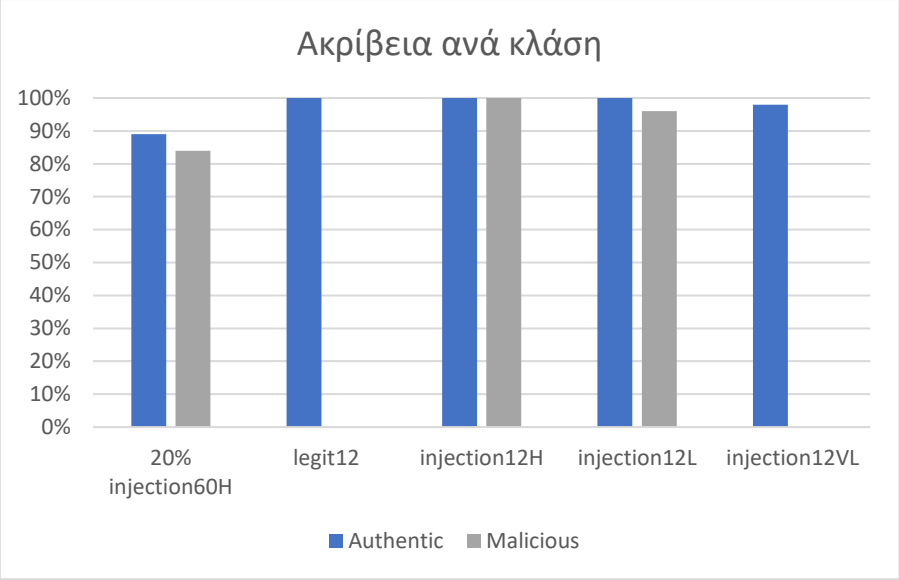
Κατά την ανίχνευση με το μοντέλο διανυσματικής ταξινόμησης υποστήριξης, παρόμοια με την επίθεση επανάληψης μηνύματος, η επιλογή του πυρήνα του μοντέλου είναι άμεση συνάρτηση του αντίστοιχου συνόλου υπό εξέταση. Στον **Πίνακας 8** παρατηρείται πως σε δεδομένα χαμηλής και πολύ χαμηλής συχνότητας επίθεσης ξεχωρίζουν ο σιγμοειδής πυρήνας και ο πυρήνας ακτινικής βάσης αντίστοιχα, ρυθμισμένοι σε κλιμακούμενη, ως προς τα χαρακτηριστικά και της διακύμανσης των δεδομένων εκπαίδευσης, τιμή της παραμέτρου γ και με κανονικοποίηση και κατάτμηση κοντά στην μονάδα. Επιπρόσθετα τα δύο αυτά μοντέλα ανταποκρίνονται και στα πειράματα με υψηλή και μηδενική συχνότητα εμφάνισης εγχύσεων πλαισίων. Στις υψηλές συχνότητες, αποδίδει η σιγμοειδής ρυθμισμένη με μοναδιαία κατάτμηση και κανονικοποίηση, ενώ στο σύνολο των αυθεντικών πλαισίων ο πυρήνας ακτινική βάσης με τις παραμέτρους αυτές

ρυθμισμένος επίσης κοντά στην μονάδα. Ο γραμμικός πυρήνας, δεν ξεχώρισε σε κάποιο πείραμα, ανταποκρίθηκε σχετικά καλά όμως στις υψηλές συχνότητες, ρυθμισμένος σε κατάτμηση και κανονικοποίηση κοντά στην μονάδα. Κατά την δοκιμή με το σύνολο εκπαίδευσης τα αποτελέσματα και με τους τρείς πυρήνες δεν ήταν ικανοποιητικά. Ενδεικτικά στον πίνακα παρουσιάζεται το καλύτερο για το σενάριο αυτό, που επιτεύχθηκε με τον πυρήνα ακτινικής βάσης.

Πίνακας 8 Αποτελέσματα πειραμάτων ανίχνευσης έγχυσης πλαισίου με SVC

Test set	**kernel**	**Accuracy**	**Precision**	**Recall**	**F1-score**
20% of	rbf	87%	89%	92%	90%
injection60H			84%	78%	81%
legit12	rbf	100%	100%	100%	100%
			0%	0%	0%
injection12H	sigmoid	100%	100%	100%	100%
			100%	100%	100%
injection12L	rbf	99%	100%	99%	99%
			96%	100%	98%
injection12VL	sigmoid	98%	98%	100%	99%
			100%	80%	89%

Μια σύγκριση των αποτελεσμάτων μπορεί να πραγματοποιηθεί με την βοήθεια της παρακάτω γραφικής παράστασης (**Διάγραμμα 5**).



Διάγραμμα 5 Αποτελέσματα πειραμάτων ανίχνευσης έγχυσης πλαισίου με SVC

6.5.2.2 Feed Forward Neural Network

Όπως και στην περίπτωση της επίθεσης επανάληψης μηνύματος, για το νευρωνικό δίκτυο χρησιμοποιήθηκαν τρία επίπεδα με μεταβλητό πλήθος νευρώνων και είδος συνάρτησης ενεργοποίησης. Η επίδοση του ήταν ελαφρώς καλύτερη από την αντίστοιχη της επανάληψης, χωρίς να ξεχωρίζει κάποιο σύνολο δοκιμής. Ορισμένα αποτελέσματα παρουσιάζονται στο **Πίνακας 9**.

Πίνακας 9 Αποτελέσματα πειραμάτων ανίχνευσης έγχυσης πλαισίου με FFNN

Test set	Accuracy	Precision	Recall	F1-score
20% of injection60H	88%	89%	94%	91%
		86%	78%	82%
injection12H	93%	96%	93%	94%
		86%	92%	89%
injection12L	87%	99%	85%	91%
		58%	95%	72%

Και στις 3 περιπτώσεις ως συνάρτηση ενεργοποίησης στο επίπεδο εισόδου και εξόδου χρησιμοποιήθηκε η Relu και η sigmoid αντίστοιχα, ως μέγεθος κατάτμησης της στήλης δεδομένων επιλέχθηκε η μονάδα και ως μέγεθος της κάθε παρτίδας (batch) το 16. Το πλήθος των επαναλήψεων διακυμάνθηκε μεταξύ του 100 και του 200 και το πλήθος των νευρώνων εισόδου μεταξύ 64 και 128.

6.5.2.3 Long Short-Term Memory

Τα πειράματα δείξαν πως η έγχυση πλαισίου με το μοντέλο αυτό δεν είναι εύκολα ανιχνεύσιμη. Εξαιρετική είναι η δυνατότητα του να ξεχωρίζει τα αυθεντικά πλαίσια, δεν μπορεί όμως να υποθεί το ίδιο και για τα κακόβουλα. Η τιμές των μετρικών κατά τα πειράματα δοκιμής στο σύνολο εκπαίδευσης και στα σύνολα μηδενικής και υψηλής συχνότητας εμφάνισης επιθέσεων, παρουσιάζονται στον ακόλουθο **Πίνακας 10**.

Πίνακας 10 Αποτελέσματα πειραμάτων ανίχνευσης έγχυσης πλαισίου με LSTM

Test set	Accuracy	Precision	Recall	F1-score
20% of	88%	92%	90%	91%
injection60H		81%	85%	83%
legit12	100%	100%	100%	100%
		0%	0%	0%
injectin12H	92%	96%	91%	94%
		84%	92%	88%

Οι τιμές επαληθεύουν την προηγούμενη παρατήρηση σχετικά με την ευαισθησία του στον εντοπισμό των αυθεντικών πλαισίων. Σημειώνεται πως στο πρώτο και το τρίτο σύνολο, η ανίχνευση είναι βασισμένη στα δεδομένα και μάλιστα κατατμημένα σε μεγέθη των 10 ή 20 Bytes αντίστοιχα, ενώ στην περίπτωση του συνόλου των αυθεντικών χρησιμοποιήθηκε υβριδική ανίχνευση με κατάτμηση των 5 Bytes.

6.5.2.4 Random Forest

Παρόμοια με το προηγούμενο μοντέλο, αυτό της μακροπρόθεσμης μνήμης *Long Short-Term Memory*, κατά την εκτέλεση των πειραμάτων παρουσιάστηκε αδυναμία στον εντοπισμό των κακόβουλων πλαισίων. Σε γενικές γραμμές η επίδοση βελτιώνονταν με την αύξηση των επαναλήψεων, *epochs*, και σε ορισμένες περιπτώσεις με την ανίχνευση βασισμένη στο χρόνο. Την καλύτερη επίδοση την εμφανίζει κατά τη δοκιμή στο σύνολο εκπαίδευσης με μικρή κατάτμηση, υβριδική ανίχνευση και μεγάλη τιμή *epochs*. Οι τιμές των μετρικών σε αυτήν την περίπτωση παρουσιάζονται στον ακόλουθο πίνακα (**Πίνακας 11**).

Πίνακας 11 Αποτελέσματα πειραμάτων ανίχνευσης έγχυσης πλαισίου με RF

Test set	Accuracy	Precision	Recall	F1-score
20% of	91%	91%	95%	93%
injection60H		89%	83%	86%

6.5.2.5 k Nearest Neighbors

Το μοντέλο των k εγγύτερων γειτόνων αποτελεί το τρίτο στη σειρά που με μεγάλη δυσκολία ανιχνεύει την επίθεση έγχυσης πλαισίου. Εξαιρετική είναι η συμπεριφορά στην αναγνώριση των αυθεντικών στα δεδομένα μηδενικής συχνότητας εμφάνισης επίθεσης, με το μοντέλο να χρησιμοποιεί μεγάλο πλήθος γειτόνων στη φάση της πρόβλεψης και μέτριου μεγέθους κατάτμηση των δεδομένων. Μια χαμηλή επίδοση παρουσίασε στις περιπτώσεις των δοκιμών στα δεδομένα εκπαίδευσης και σε αυτά της υψηλής πιθανότητας εμφάνισης επιθέσεων, στα οποία το μοντέλο ρυθμίστηκε με τον ίδιο τρόπο, χρησιμοποιώντας μικρό πλήθος γειτόνων και μικρό μέγεθος κατάτμησης των δεδομένων. Σε κάθε άλλη περίπτωση οι μετρικές δείξαν αποτυχία του μοντέλου. Τα αποτελέσματα των τριών αυτών πειραμάτων μπορούν να βρεθούν στον ακόλουθο πίνακα (**Πίνακας 12**).

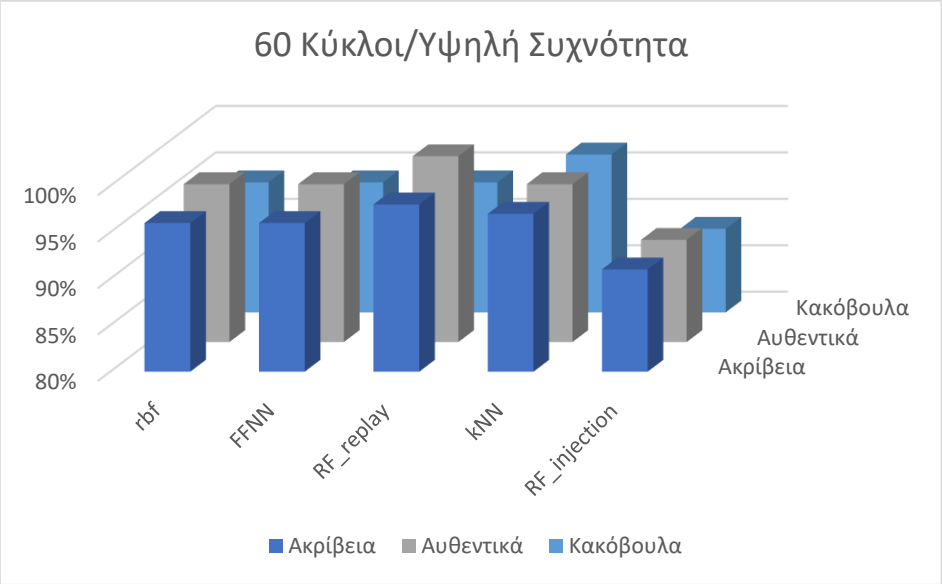
Πίνακας 12 Αποτελέσματα πειραμάτων ανίχνευσης έγχυσης πλαισίου με kNN

Test set	Accuracy	Precision	Recall	F1-score
20% of	86%	90%	90%	90%
injection60H		80%	80%	80%
legit12	92%	100%	92%	96%
		0%	0%	0%
injection12H	89%	90%	94%	92%
		86%	79%	83%

6.6 Σχολιασμός

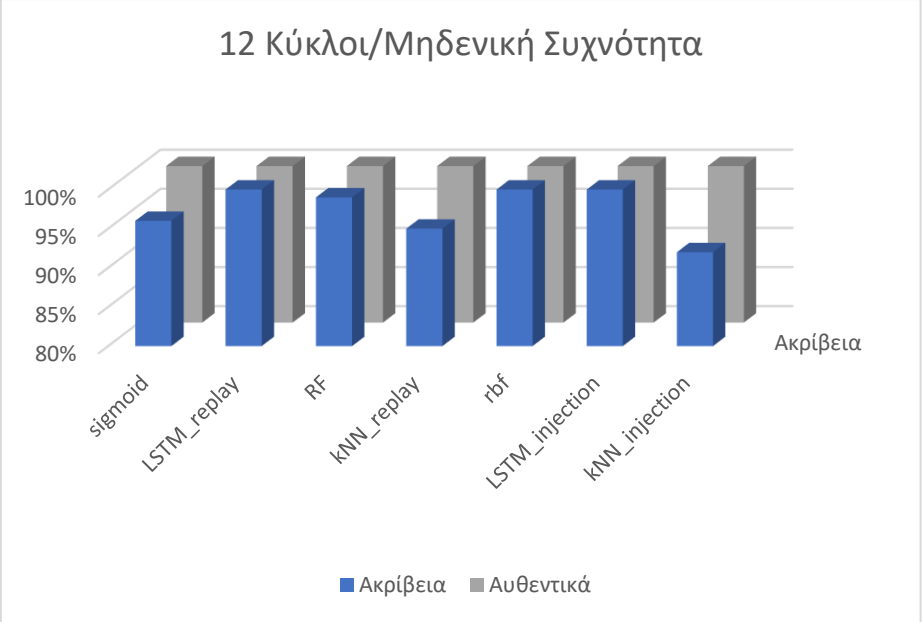
Κατά την δοκιμή στο σύνολο εκπαίδευσης η ανίχνευση των επιθέσεων επανάληψης μπορούν να πραγματοποιηθούν με τα μοντέλα SVC rbf, FFNN, RF και kNN ενώ για τις αντίστοιχες της έγχυσης προτείνεται το RF. Οι ακρίβειες των μοντέλων, όπως φαίνεται

στο **Διάγραμμα 6**, κυμαίνονται από 91% έως 98% με τις επιμέρους ακρίβειες των κλάσεων ταξινόμησης μεταξύ 89% και 100%.



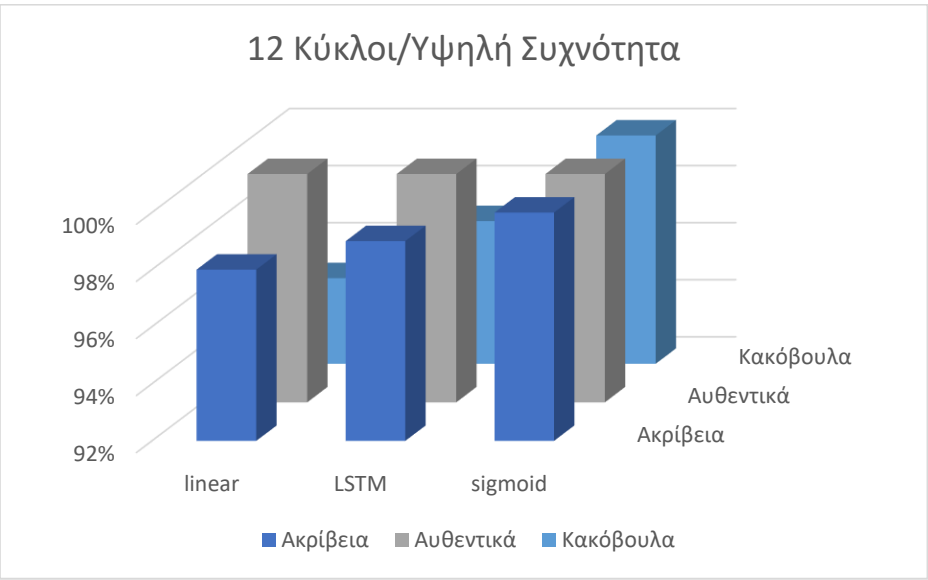
Διάγραμμα 6 Σύγκριση πειραμάτων ανίχνευσης σε σύνολο δεδομένων 60 κύκλων και υψηλής συχνότητας

Στην περίπτωση των αυθεντικών σε σύνολο μηδενικής πιθανότητας εμφάνισης κακόβουλων πλαισίων οι επιλογές και για τους δύο τύπους επίθεσης είναι αρκετοί. Η ανίχνευση της επανάληψης πλαισίου επιτυγχάνεται με τα SVC sigmoid, LSTM, RF, kNN με ποσοστά ακρίβειας από 96% έως και 100%. Ομοίως στις επιθέσεις έγχυσης επιλέγονται τα μοντέλα SVC rbf, LSTM, kNN με ποσοστά ακρίβειας από 92% έως και 100%. Οι ακριβείς επιδόσεις μπορούν αν παρατηρηθούν στο **Διάγραμμα 7**.



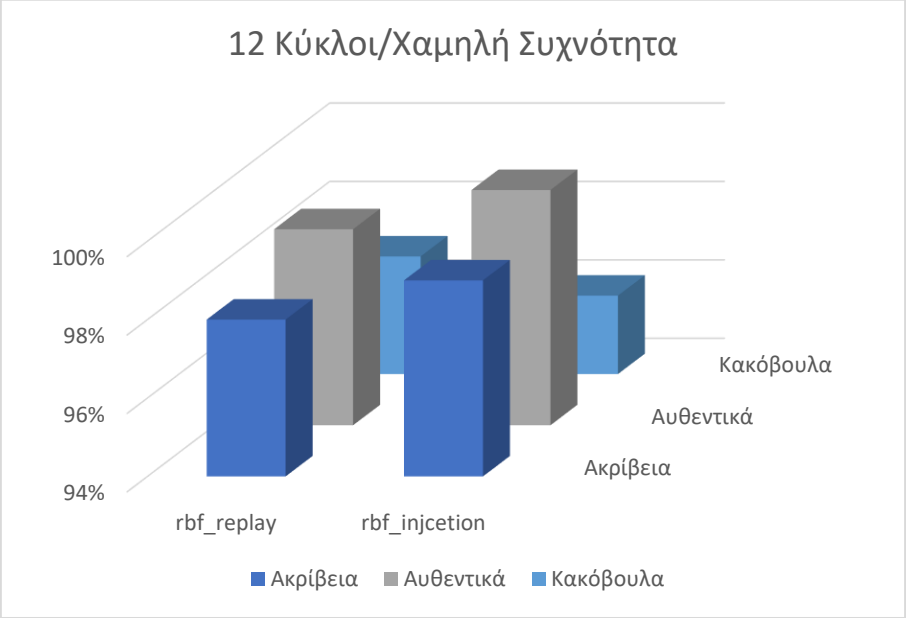
Διάγραμμα 7 Σύγκριση πειραμάτων ανίχνευσης σε σύνολο δεδομένων 12 κύκλων και μηδενικής συχνότητας

Η επιλογή μοντέλου ανίχνευσης επιθέσεων υψηλής συχνότητας σε μικρό πλήθος δεδομένων, είναι περιορισμένη. Στην επανάληψη πλαισίου ανταποκρίνονται τα SVC linear και LSTM ενώ στην έγχυση μόνο το SVC sigmoid. Βέβαια παρά το περιορισμό αυτόν, οι επιδόσεις και των τριών είναι εξαιρετικές όπως φαίνεται και στο ακόλουθο διάγραμμα (**Διάγραμμα 8**).

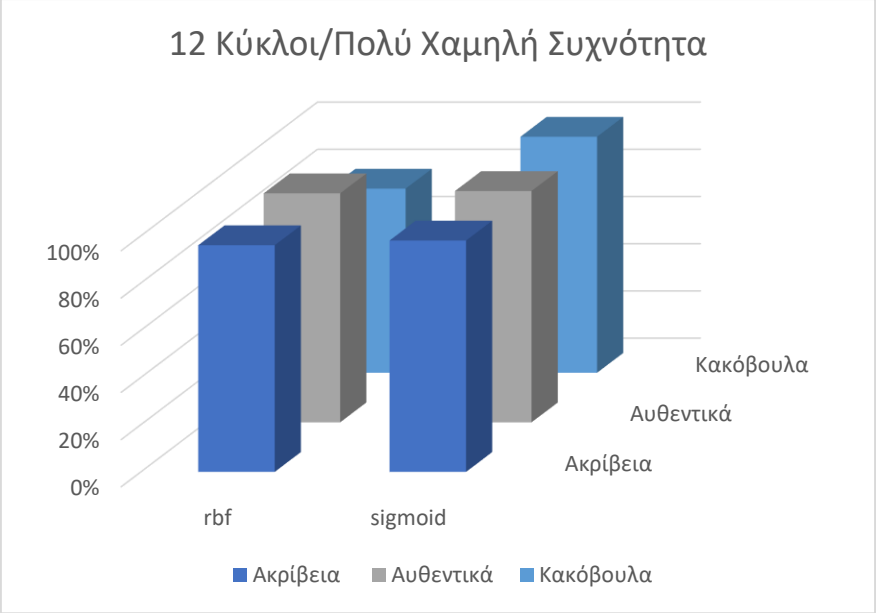


Διάγραμμα 8 Σύγκριση πειραμάτων ανίχνευσης σε σύνολο δεδομένων 12 κύκλων και υψηλής συχνότητας

Η ανίχνευση επιθέσεων χαμηλής και πολύ χαμηλής συχνότητας, όπως φαίνεται στα διαγράμματα **Διάγραμμα 9** και **Διάγραμμα 10**, είναι αποκλειστική υπόθεση του μοντέλου ταξινόμησης με διάνυσμα υποστήριξης. Κατά την επανάληψη πλαισίου ο μόνος πυρήνας που ανταποκρίνεται είναι αυτός της ακτινικής βάσης, με εξαιρετική επίδοση στις χαμηλές συχνότητες, όχι όμως τόσο ικανοποιητική στις πολύ χαμηλές. Στην περίπτωση της έγχυσης επίσης στις χαμηλές συχνότητες επιλέγεται ο πυρήνας ακτινικής βάσης, στις πολύ χαμηλές όμως μονόδρομος είναι ο σιγμοειδής.



Διάγραμμα 9 Σύγκριση πειραμάτων ανίχνευσης σε σύνολο δεδομένων 12 κύκλων και χαμηλής συχνότητας



Διάγραμμα 10 Σύγκριση πειραμάτων ανίχνευσης σε σύνολο δεδομένων 12 κύκλων και πολύ χαμηλής συχνότητας

Συνοψίζοντας τα αποτελέσματα των πειραμάτων παρατηρείται πως μειώνοντας την συχνότητα εμφάνισης επιθέσεων ανεξάρτητα αν πρόκειται για επανάληψη πλαισίου ή έγχυση πλαισίου, οι διαθέσιμες επιλογές περιορίζονται σταδιακά στο SVC και μάλιστα με kernels των σιγμοειδή και της ακτινική βάσης. Αυτό οφείλεται στην ευελιξία των δύο αυτών kernels να προσαρμόζουν το decision boundary σε σύνολα δεδομένων μη ισορροπημένα ως προς τα δείγματα της κάθε κλάσης και δείχνει πως μειώνοντας την συχνότητα στα δεδομένα, αυτά τείνουν να γίνουν μη γραμμικά διαχωρίσιμα. Επιπρόσθετα τα μοντέλα στην πλειοψηφία τους φαίνεται να εξυπηρετούνται με την κατάτμηση των δεδομένων και με την υβριδική ανίχνευση. Ταυτόχρονα φαίνεται πως η ανίχνευση της επίθεσης επανάληψης είναι πιο εύκολη ενώ αυτή της έγχυση πιο απαιτητική. Κοινές συμπεριφορές των μοντέλων παρατηρούνται ανάμεσα στις δύο κατηγορίες επιθέσεων και των αντίστοιχων συχνοτήτων εμφάνισης τους.

7. Συμπεράσματα

7.1 Σύνοψη

Στην παρούσα διπλωματική μελετήθηκε το ζήτημα της κυβερνοασφάλειας των ευφυών και συνδεδεμένων οχημάτων. Προσδιορίστηκε ο όρος και αναδείχθηκε η σπουδαιότητα και η σημασία της ύπαρξης διαφάνειας και ασφάλειας. Επιλέχθηκε και μελετήθηκε ένα από τα πιο διαδεδομένα και ελπιδοφόρα για τον χώρο αυτόν πρωτόκολλα ενδοεπικοινωνίας, το FlexRay, και παρουσιάστηκαν οι τρόποι με τους οποίες μπορεί αυτό να προσβληθεί και να εξυπηρετήσει κακόβουλους σκοπούς. Συνοψίστηκαν οι κύριες υπηρεσίες αυτού και περιγράφηκε ο τρόπος με τον οποίο λειτουργεί. Η εργασία ξεχωρίζει από την διαθέσιμη βιβλιογραφία, καθώς μελετά την ανάπτυξη ενός εργαλείου ανίχνευσης επιθέσεων στο επίπεδο της διασύνδεσης των δεδομένων του δικτύου και προσφέρει σε αυτήν ένα σύνολο πειραμάτων και αποτελεσμάτων με διαφορετικά μοντέλα. Ταυτόχρονα όμως, αναντίρρητη είναι και η προσφορά ενός λογισμικού προσομοίωσης του πρωτοκόλλου, το οποίο υποστηρίζει ένα πλήθος μηχανισμών και λειτουργιών αυτού. Λαμβάνοντας υπόψιν το πειραματικό περιβάλλον, τις ευπάθειες και τα διανύσματα επίθεσης του πρωτοκόλλου αλλά και την μελέτη στο αντικείμενο της ανίχνευσης και ασφάλειας το υπό μελέτη σύστημα αφορά ένα μικρό μέρος μιας επικοινωνίας FlexRay, η οποία έχει δεχτεί μια σειρά από επιθέσεις πλήρως επιτυχημένες, με ελάχιστα περιθώρια ανίχνευσης της με γυμνό οφθαλμό ή συμβατικούς μεθόδους ελέγχου των κανόνων του πρωτοκόλλου. Πρόκειται για μια περίπτωση που για να προκύψει, κυρίως λόγο της ντετερμινιστικότητας και της προ-διαμόρφωσης της πλειοψηφίας των παραμέτρων από τον αρχιτέκτονα του δικτύου, απαιτεί επιτιθέμενους με γνώσεις και προηγμένα εργαλεία αλγορίθμων. Από τα αποτελέσματα, λοιπόν είναι εύληπτα αντιληπτό πως η ανίχνευση στο αμέσως επόμενο επίπεδο του δικτύου μετά το φυσικό, είναι δυνατή και πως η παρούσα διπλωματική αποτελεί μια απόδειξη πως ένα πολύεπίπεδο σύστημα ανίχνευσης είναι πιθανό να αποδώσει καρπούς και να βοηθήσει στην εξιχνίαση και αποτροπή εγκληματικών ενεργειών. Παράλληλα αναντίρρητα αποτελεί ενθαρρυντικό παράγοντα για την ενίσχυση της προστασίας των ευφυών και συνδεδεμένων οχημάτων και την δημιουργία πιο ασφαλών τεχνολογιών.

7.2 Μελλοντικές επεκτάσεις

Η επέκταση και συνέχιση της παρούσας διπλωματικής εγείρει το ενδιαφέρον σε δύο επίπεδα. Το πρώτο αφορά το λογισμικό προσομοίωσης. Οι λειτουργίες και μηχανισμοί που υλοποιήθηκαν αποτελούν ένα πολύ μικρό μέρος των δυνατοτήτων και υπηρεσιών του πρωτοκόλλου. Αρχικά μπορεί να υποστηριχθεί το δυναμικό μέρος του κύκλου επικοινωνίας και άρα η πυροδοτούμενη από γεγονότα φύση του πρωτοκόλλου. Εν συνεχεία μπορούν να προστεθούν παραπάνω κόμβοι, να δημιουργηθούν οι τοπολογίες του FlexRay και να προστεθεί το κανάλι B, δίνοντας την δυνατότητα για προσθήκη και μελέτη επιπλέον επιθέσεων, όπως η άρνηση παροχής υπηρεσιών, και για υποστήριξη περισσότερων υπηρεσιών, όπως οι καταστάσεις σφάλματος των κόμβων. Ένα τέτοιο μέσο θα ενθαρρύνει την επιστημονική κοινότητα να στραφεί στην μελέτη του πρωτοκόλλου αυτού και την δημοσίευση πολλών περισσότερων πορισμάτων για την ασφάλεια του. Το δεύτερο επίπεδο αφορά φυσικά στην ανίχνευση. Υπάρχουν πολλά μοντέλα προς δοκιμή και κυρίως μηχανισμοί ανίχνευσης και άμυνας. Σε συνδυασμό με το πρόγραμμα προσομοίωσής μπορεί να δημιουργηθεί μια διεπαφή για δοκιμή ακόμα και σε πραγματικό χρόνο των επιλεγμένων μεθόδων. Επιπρόσθετα αντίστοιχη διεπαφή μπορεί να σχεδιαστεί και με λογισμικά επαλήθευσης υλικού και έτσι οι μηχανισμοί ανίχνευσης να υλοποιηθούν και δοκιμαστούν ακόμα και σε γλώσσες περιγραφή υλικού, συνθέτοντας έτσι ένα ολοκληρωμένο προϊόν.

Βιβλιογραφία

[1] Markus Iversen Huse, *FlexRay Analysis, Configuration Parameter Estimation, and Adversaries*. Norwegian university of Science and Technology (NTNU), 2017

[2] FlexRay™, *FlexRay Communications System Protocol Specification Version 3.0.1*. 2010

[3] Irdin Pekaric, Clemens Sauerwein, Stefan Haselwanter, Michael Felderer, *A taxonomy of attack mechanisms in the automotive domain*, Elsevier, 2021

[4] Patrick McClanahan, *Information Security*, San Joaquin Delta College, LibreTexts, 2023

[5] Jiajia Liu, Abderrahim Benslimane, *Intelligent and Connected Vehicle Security*, River Publishers, 2021

[6] Nicolas Navet, Francoise Simonot-Lion, *Automotive Embedded Systems Handbook*, CRC Press, 2009

[7] Takeshi Kishikawa, Ryo Hirano, Yoshihiro Ujiie, Tomoyuki Haga, Hideki Matsushima, Kazuya Fujimura, Jun Anzai, *Vulnerability of FlexRay and Countermeasures*, SAE International, 2019

[8] Pal-Stefan Murvay, Bogdan Groza, Practical Security Exploits of the FlexRay in-vehicle communication protocol, Politehnica University of Timisoara, Romania

[9] Texas Instruments, *FlexRay Module Training - TI Safety Microcontroller*, 2015

[10] Dominique Paret, *FlexRay and its Applications - Real-time Multiplexed Networks*, WILEY, 2012, ISBN: 9781119979562

[11] Sampath Rajapaksha, Harsa kalutarage, M. Omar Al-Kadri, Andrei Petrovski, Garikayi Madzudzo, Madeline Cheah, *AI-Based Intrusion Detection Systems for In-Vehicle Networks: A Survey*, ACM Computing Surveys, 2023

[12] Mahdi Dibaei, Xi Zheng, Kun Jiang, Sasa Maric, Robert Abbas, Shigang Liu, Yuexin Zhang, Yao Deng, Sheng Wen, Jun Zhang, Yang Xiang, and Shui Yu, *An Overview of Attacks and Defences on Intelligent Connected Vehicles*, 2019

[13] NXP Semiconductors, *MPC5744P FlexRay Interface in Pictures – Application Note*, 2021

[14] Tian Guan, Yi Han, Nan Kang, Ningye Tang, Xu Chen, Shu Wang, *An overview of Vehicular Cybersecurity for Intelligent Connected Vehicles*, MDPI, 2022

[15] Nevrus Kaja, *Artificial Intelligence and Cybersecurity: Building an Automotive Cybersecurity Framework Using Machine Learning Algorithms*, University of Michigan-Dearborn, 2019

[16] *Cyber Security and Resilience of smart cars – Good practices and recommendations*, European Union Agency for Network And Information Security (ENISA), 2016

[17] Bifta Sama Bari, Kumar Yelamarthi, Sheikh Ghafoor, *Intrusion Detection in Vehicle Controller Area Network (CAN) Bus Using Machine Learning: A Comparative Performance Study*, MDPI, 2023

[18] Ajeet Kumar Dwivedi, *Anomaly Detection in Intra-Vehivle Networks*, Western university, London, Ontario, Canada, 2022

[19] Pengzhou Cheng, Mu Han, Gongshen Liu, *DESC-IDS: Towards an efficient real-time automotive intrusion detection system based on deep envolvin stream clustering*, ELSEVIER, 2023

[20] Khaled Karray, *Cyber-security of Connected Vehicles - Contributions to enhance the Risk Analysis and Security of in-Vehicle Communications*, Universite Paris-Saclay, Telecom Paris Tech, 2019

[21] Damien Stolarz, *Car PC Hacks Tips & Tools for Geeking your Ride*, O'Reilly, 2005, ISBN: 0-596-00871-6

[22] Lin Tong, Chen Luhai, *Common Attacks Against Car Infotainment Systems*, Automotive Linux Summit, Intel, 2019

[23] Bhavesh Raju Mudhivarthi, Prabhat Thakur, Ghanshyam Singh, *Aspects of Cyber Security in Autonomous and Connected Vehicles*, MDPI, 2023

[24] Emad Aliwa, Omer Rana, Charith Perera, Peter Burnap, *Cyberattacks and Countermeasures for In-Vehicle Networks*, ResearchGate, 2020

[25] Rajkumar Singh Rathore, Chaminda Hewage, Ommprakash Kaiwartya, Jaime Lloret, *In-Vehicle Communication Cyber Security: Challenges and Solutions*, MDPI, 2022

[26] Zeinab El-Rewini, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, Prakash Ranganathan, *Cybersecurity challenges in vehicular communications*, ELSEVIER, 2019

[27] Cabell Hodge, Konrad Hauck, Shivam Gupta, Jesse Bennet*, Vehicle Cybersecurity Threats and Mitigation Approaches*, National Renewable Energy laboratory (NREL), 2019

[28] Roberto Passerone, Daniela Cancila, Michele Albano, Sebti Mouelhi, Sandor Plosz, Epkki Jantunen, Anna Ryabokon, Emine Laarouchi, Csaba Hegedus, Pal Varga, *A Methodology for the Design of Safety-Compliant and Secure Communication of Autonomous Vehicles*, IEEE Access, 2019

[29] Tamas Becsi, Szilard Aradi, Peter Gaspar, *Security Issues and Vulnerabilities in Connected Car Systems*, Models and Technologies for Intelligent Transportation Systems (MT-ITS), Budapest, Hungary, 2015

[30] Numaan Huq, Craig Gibson, Vladimir Kropotov, Rainer Vosseler, *Cybersecurity for Connected Cars- Exploring Risks in 5G, Cloud and Other Connected Technologies*, Trend Micro Research, 2017

[31] Eric Armengaud and Andreas Steininger, Martin Horauer, *Automatic Parameter Identification in FlexRay based Automotive Communication Networks*, IEEE, 2006

[32] Ruey-Kai Sheu, Mayuresh Sunil Pardeshi, Lun-Chi Chen, *Autonomous Mutual Authentication Protocol in the Edge Networks*, MDPI, 2022

[33] Zdenek Hanzalek, David Benes, Scheduling of the FlexRay communication protocol respecting AUTOSAR FlexRay Com stack, Czech Technical University in Prague

[34] Georg Macher, Christoph Schmittner, Omar Veledar, Eugen Brenner*, ISO/SAE DIS 21434 Automotive Cybersecurity Standard – In a Nutshell*, Institute of Technical Informatics, Graz University of Technology

[35] Brandon Barry, *Making Sense of Security Testing for ISO/SAE 21434 & UNR 155*, Block Harbor Cybersecurity, 2019

[36] Philipp Veronesi, Manuel Sandler, *Automotive Cybersecurity-The Essential Guide to ISO/SAE 21434-How to manage the challenges of the new automotive cybersecurity standards and regulations*, CYRES Consulting

[37] Vit Sembera, *ISO/SAE 21434 Setting the Standard for Connected Cars Cybersecurity*, Trend Micro Research

[38] Alexander Palm, Benjamin Gafvelin, *Ethical Hacking of Android Auto in the Context of Road Safety*, KTH Vetenskap Och Konst, Stockholm, 2021

[39] Yeonghum Shin, Sungbum Kim, Wooyeon Jo, Taeshik Shon, *Digital Forensic Case Studies for In-Vehicle Infotainment Systems Using Android Auto and Apple CarPlay*, MDPI, 2022

[40] Mert Pese, Kang Shin, Josiah Bruner, Amy Chu, *Security Analysis of Android Automotive*, SAE International, 2020

[41] Vishnu Renganathan, Ekim Yurtsever, Qadeer Ahmed, Aylin Yener, *Valet attack on privacy: a cybersecurity threat in automotive Bluetooth infotainment systems*, Springer Open, 2022

[42] Amit Kr Mandal, Agostino Cortesi, Pietro Ferrara, Federica Panarotto, Fausto Spoto, *Vulnerability Analysis of Android Auto Infotainment Apps*, Ischia, Italy, Association for Computing Machinery, 2018

[43] Jin-Hui Piao, Yu-Jing Wu, Yi-Nan Xu, *A Security Framework for In-Vehicle FlexRay Bus Network*, International Journal of Modeling and Optimization, 2022

[44] Vahid Lari, Mehdi Dehbashi, Seyed Ghassem Miremadi, Navid Farazmand, *Assessment of Message Missing Failures in FlexRay-Based Networks*, Sharif University of Technology, 13th IEEE international Symposium on pacific Rim Dependable Computing, 2007

[45] Trong-Yen Lee, I-An Lin, Ren-Hong Liao, *Design of a FlexRay/Ethernet Gateway and Security Mechanism for In-Vehicle Networks*, MDPI, 2019

[46] Mehdi Dehbashi, Vahid Lari, Seyed Ghassem Miremadi, Mohammad Shokrollah-Shirazi, *Fault Effects in FlexRay-Based Networks with Hybrid Topology*, Sharif university of Technology, The Third international Conference on Availability, Reliability and Security, 2008

[47] Takeshi Kishikawa, Ryo Hirano, Yoshihiro Ujiie, Tomoyuki Haga, Hideki Matsushima, Kazuya Fujimura, Jun Anzai, *Intrusion Detection and Prevention System for FlexRay against Spoofed Frame Injection*, Panasonic Corporation, Japan, 2019

[48] Omar Y. Al-Jarrah, Carsten Maple, Mehrdad Dianati, David Oxtoby, Alex Mouzakitis, *Intrusion Detection Systems for Intra-Vehicle Networks: A Review*, IEEE Access, 2019

[49] Georgios Karopoulos, Georgios Kambourakis, Efstratios Chatzoglou, Jose Luis Hernadez Ramos, *Demystifying In-Vehicle Intrusion Detection Systems: A Survey of Surveys and a Meta-Taxonomy*, MDPI, 2022

[50] Paula Vasile, Bogdan Groza, Stefan Murvay, *Performance analysis of broadcast authentication protocols on CAN-FD and FlexRay*, Politehnica University of Timisoara, Timisoara, Romania, 2015

[51] Gang Han, Haibo Zeng, Yaping Li, Wnhua Dou, *SAFE: Security-Aware FlexRay Scheduling Engine*, IEEE Xplore, 2014 EDAA

[52] Ishtiaq Rouf, Rob Miller, Hossen Mustafa, Travis Taylor, Sangho Oh, Wnyuan Xu, Marco Gruteser, Wade Trappe, Ivan Seskar, *Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring Systems Case Study*, US National Science Foundation and Army Reseatch Office, 2010

[53] Zhendong Wang, Haoran Wei, Jianda Wang, Xiaoming Zeng, Yuchao Chang, *Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey*, MDPI, 2022

[54] Craig Smith, *Car Hacker's Handbook-A Guide for the Penetration Test*, No Starch Press, 2016

[55] Shiho Kim, Rakesh Shrestha, *Automotive Cyber Security – Introduction, Challenges, and Standardization*, Springer, 2020

[56] Dominique Paret, Multiplexed Networks for Embedded Systems-CAN, LIN, FlexRay, Safe-by-Wire, WILEY, 2005

[57] Masashi Tanaka, Junko Takahashi, Yoshihito Oshima, *Cyber-attack Countermeasures for Cars*, NTT Technical Review, 2017

[58] Prinkle Sharma, James Gillanders, *Cybersecurity and Forensics in Connected Autonomous Vehicles: A Review of the State-of-the-Art*, IEEE Access, 2022

[59] Himanshu Thapliyal, Saraju P. Mohanty, Stacy Prowell, *Emerging Paradigms in Vehicular Cybersecurity*, IEEE Consumer Electronics Magazine, 2019

[60] Hohn N. Brewer, George Dimitoglou, *Evaluation of Attack Vectors and Risks in Automobiles and Road Infrastructure*, IEEE CSCI, 2019

[61] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, *Experimental Security Analysis of a Modern Automobile*, IEEE Symposium on Security and Privacy, 2010

[62] Narayan Kharti, Rakesh Shrestha, Seung Yeob Nam, *Security Issues with In-Vehicle Networks, and Enhanced Countermeasures Based on Blockchain*, MDPI, 2021

[63] Martin Horauer, Oliver praprotnik, Martin Zauner, Roland Holler, Paul Milbredt, *A Test Toll for FlexRay-based Embedded Systems*, IEEE, 2007

[64] Eric Armengaud, Andreas Steininger, Hannes Friedl, Roman Pallierer, *An FPGA based SoC Design for Testing Embedded Automotive Communication Systems employing the FlexRay Protocol*, CiteSeerX, 2004

[65] Giampaolo Bella, Pietro Biondi, Gianpiero Constantino, Ilaria Matteucci, *Designing and implementing an AUTOSAR-based Basic Software Module for enhanced security*, ELSEVIER, 2022

[66] Thien-Nu Hoang, Daehee Kim, *Detecting in-vehicle intrusion via semi-supervised learning-based convolutional adversarial autoencoders*, ELSEVIER, 2022

[67] Camil Jichici, Bogdan Groza, Pal-Stefan Murvay, *Examining the Use of Neural Networks for Intrusion Detection in Controller Area Networks*, SPRINGER, 2018

[68] Camil Jichici, Bogdan Groza, Pal-Stefan Murvay, *Integrating Adversary Models and Intrusion Detection Systems for In-Vehicle Networks in CANoe*, SPRINGER, 2019

[69] Wu Yan, Wang Lifang, Liao Chenglin, Li Fang, *In-Vehicle FlexRay Bus Monitoring System*, ITEC Asia-Pacific, 2014

[70] Alfonso Martínez-Cruz, Kelsey A. Ramírez-Gutiérrez, Claudia Feregrino-Uribe, Alicia Morales-Reyes, *Security on in-vehicle communication protocols: Issues, challenges, and future research directions*, ELSEVIER, 2021

[71] Shiyi Jin, Jin-Gyun Chung, Yinan Xu, *Signature-Based Intrusion Detection System (IDS) for In-Vehicle CAN Bus Network*, IEEE Xplore, 2023

[72] Andriy Burkov, *The Hundred-Page Machine Learning Book*, 2019

[73] Sakib Ashraf Zargar, *Introduction to Sequence Learning Models: RNN, LSTM, GRU*, Department of Mechanical and Aerospace Engineering, North Carolina State University, Raleigh, North Carolina, USA, 2021

[74] Saikat Dutt, Subramanian Chandramouli, Amit Kumar Das, *Machine Learning*, Pearson, 2019